

Barricade 2.4 GHz 11 Mbps Wireless Cable/DSL Broadband Router

User Guide

SMC7004VWBR



Barricade™ 2.4 GHz 11 Mbps Wireless Cable/DSL Broadband Router User Guide

From SMC's Barricade line of Broadband Routers

SMC®

Networks

38 Tesla

Irvine, CA 92618

Phone: (949) 679-8000

May 2003

Pub. # 150000026400E

COPYRIGHT

Information furnished by SMC Networks, Inc. (SMC) is believed to be accurate and reliable. However, no responsibility is assumed by SMC for its use, nor for any infringements of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent or patent rights of SMC. SMC reserves the right to change specifications at any time without notice.

Copyright © 2003 by
SMC Networks, Inc.
38 Tesla
Irvine, CA 92618

All rights reserved. Printed in Taiwan

Trademarks:

SMC is a registered trademark; and Barricade is a trademark of SMC Networks, Inc. Other product and company names are trademarks or registered trademarks of their respective holders.

COMPLIANCES

FCC - Class B

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with instructions, may cause harmful interference to radio communications. However, there is no guarantee that the interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient the receiving antenna
- Increase the separation between the equipment and receiver
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
- Consult the dealer or an experienced radio/TV technician for help

FCC Caution: To assure continued compliance, (example - use only shielded interface cables when connecting to computer or peripheral devices) any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

IMPORTANT NOTE: FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Industry Canada - Class B

This digital apparatus does not exceed the Class B limits for radio noise emissions from digital apparatus as set out in the interference-causing equipment standard entitled "Digital Apparatus," ICES-003 of the Department of Communications.

Cet appareil numérique respecte les limites de bruits radioélectriques applicables aux appareils numériques de Classe B prescrites dans la norme sur le matériel brouilleur: "Appareils Numériques," NMB-003 édictée par le ministère des Communications.

EC Conformance Declaration - Class B

SMC contact for these products in Europe is:

SMC Networks Europe,
Edificio Conata II,
Calle Frutuós Gelabert 6-8, 2^o, 4^a,
08970 - Sant Joan Despí,
Barcelona, Spain.

This information technology equipment complies with the requirements of the Council Directive 89/336/EEC on the Approximation of the laws of the Member States relating to Electromagnetic Compatibility and 73/23/EEC for electrical equipment used within certain voltage limits and the Amendment Directive 93/68/EEC. For the evaluation of the compliance with these Directives, the following standards were applied:

- RFI * Limit class B according to EN 55022:1998
- Emission:* Limit class B for harmonic current emission according to EN 61000-3-2:1995
 - * Limitation of voltage fluctuation and flicker in low-voltage supply system according to EN 61000-3-3:1995
- Immunity:* Product family standard according to EN 55024:1998
 - * Electrostatic Discharge according to EN 61000-4-2:1995 (Contact Discharge: ± 4 kV, Air Discharge: ± 8 kV)
 - * Radio-frequency electromagnetic field according to EN 61000-4-3: 1996 (80 - 1000 MHz with 1 kHz AM 80% Modulation: 3 V/m)
 - * Electrical fast transient/burst according to EN 61000-4-4:1995(AC/DC power supply: ± 1 kV, Data/Signal lines: ± 0.5 kV)
 - * Surge immunity test according to EN 61000-4-5:1995(AC/DC Line to Line: ± 1 kV, AC/DC Line to Earth: ± 2 kV)
 - * Immunity to conducted disturbances, Induced by radio-frequency fields: EN 61000-4-6:1996(0.15 - 80 MHz with 1 kHz AM 80% Modulation: 3 V/m)
 - * Power frequency magnetic field immunity test according to EN 61000-4-8:1993(1 A/m at frequency 50 Hz)
 - * Voltage dips, short interruptions and voltage variations immunity test according to EN 61000-4-11:1994(>95% Reduction @ 10 ms, 30% Reduction @ 500 ms, >95% Reduction @ 5000 ms)
- LVD: * EN60950(A1/1992; A2/1993; A3/1993; A4/1995; A11/1997)

TABLE OF CONTENTS

About the Wireless Barricade Router	1
LED Indicators	1
Features and Benefits	2
Installing the Wireless Barricade Router	3
Package Contents	3
Hardware Description	4
System Requirements	6
Connect the System	7
Basic Installation Procedure	7
Configuring Client TCP/IP	11
Installing TCP/IP	11
Windows 95/98/Me	11
Windows 2000	12
Setting Up TCP/IP	13
Configuring Your Computer in Windows 95/98/Me	14
Verifying Your TCP/IP Connection	24
Configuring the Wireless Barricade Router	25
Browser Configuration	25
Disable Proxy Connection	26
Internet Explorer (5 or above)	26
Internet Explorer (For Macintosh)	26
Netscape (4 or above)	27
Navigating the Web Browser Interface	28
Making Configuration Changes	28
Setup Wizard	29
Time Zone	29
Broadband Type	29
Advanced Setup	33
System	35
WAN	37
LAN	44
Wireless	45

TABLE OF CONTENTS

Network Address Translation (NAT) 48

Firewall 51

DDNS (Dynamic DNS) Settings 59

UPnP (Universal Plug and Play) Setting 60

Tools 61

Status 64

Troubleshooting65

Specifications69

ABOUT THE WIRELESS BARRICADE ROUTER

Congratulations on your purchase of the Wireless Barricade™ Broadband Router. SMC is proud to provide you with a powerful yet simple communication device for connecting your local area network (LAN) to the Internet.

LED Indicators

The SMC7004VWBR includes status LED indicators, as described in the following figure and table.



LED	Status	Description
PWR (Green)	On	The Wireless Barricade is receiving power.
WLAN (Green)	On	The Wireless Barricade has established a valid wireless connection.
WAN (Green)	On	The WAN port has established a valid network connection.
Link/ACT (Green)	On	The indicated LAN port has established a valid network connection.
	Flashing	The indicated LAN port is transmitting or receiving traffic.
Speed (Amber)	Off	The indicated LAN port has established a valid 10 Mbps network connection.
	On	The indicated LAN port has established a valid 100 Mbps network connection.

Features and Benefits

- Internet connection to DSL or cable modem via a 10/100 Mbps WAN port
- Local network connection via 10/100 Mbps Ethernet ports or 11 Mbps wireless interface (supporting up to 253 users)
- 802.11b compliant – interoperable with multiple vendors
- Provides seamless roaming within 802.11b WLAN environment
- Local network connection via 10/100 Mbps Ethernet ports
- DHCP for dynamic IP configuration, and DNS for domain name mapping
- Stateful Packet Inspection (SPI) firewall with client privileges, hacker prevention, and NAT
- NAT also enables multi-user access with a single-user account, and virtual server functionality (providing protected access to Internet services such as Web, FTP, mail and Telnet)
- Virtual Private Network (VPN) support using PPTP, L2TP or IPSec pass-through
- User-definable application sensing tunnel supports applications requiring multiple connections
- Easy setup through a Web browser on any operating system that supports TCP/IP
- Compatible with all popular Internet applications

INSTALLING THE WIRELESS BARRICADE ROUTER

Before installing the Wireless Barricade™ Broadband Router, verify that you have all the items listed under “Package Contents.” If any of the items are missing or damaged, contact your local SMC distributor. Also be sure that you have all the necessary cabling before installing the Wireless Barricade. After installing the Wireless Barricade, refer to the Web-based configuration program in “Configuring the Wireless Barricade Router” on page 25 for information on configuring the Wireless Barricade.

Package Contents

After unpacking the Barricade™ Wireless Broadband Router, check the contents of the box to be sure you have received the following components:

- Wireless Barricade Broadband Router
- Power adapter
- One CAT-5 Ethernet cable
- Four rubber feet
- Installation CD containing this User Guide and EZ 3-Click Installation Wizard
- Quick Installation Guide

Immediately inform your dealer in the event of any incorrect, missing or damaged parts. If possible, please retain the carton and original packing materials in case there is a need to return the product.

Hardware Description

The Wireless Barricade can be connected to the Internet using its RJ-45 WAN port . It can be connected directly to your PC or to a local area network using any of the Fast Ethernet LAN ports.

Access speed to the Internet depends on your service type. Full-rate ADSL can provide up to 8 Mbps downstream and 640 Kbps upstream. G.lite (or splitterless) ADSL provides up to 1.5 Mbps downstream and 512 Kbps upstream. Cable modems can provide up to 36 Mbps downstream and 2 Mbps upstream. ISDN can provide up to 128 Kbps when using two bearer channels. PSTN analog connections can now run up to 56 Kbps. However, you should note that the actual rate provided by specific service providers may vary dramatically from these upper limits.

Although access speed to the Internet is determined by the modem type connected to your Router, data passing between devices connected to your local area network can run up to 100 Mbps over the Fast Ethernet ports.

The Wireless Barricade includes an LED display on the front panel for system power and port indications that simplifies installation and network troubleshooting. It also provides 4 RJ-45 LAN ports on the front panel, as well as one RJ-45 WAN port. Full-duplex communications allow data to be sent and received simultaneously, doubling the effective throughput.

Hardware Description

- 4 RJ-45 ports for connection to a 10BASE-T/100BASE-TX Ethernet Local Area Network (LAN). These ports can auto-negotiate the operating speed to 10/100 Mbps, the mode to half/full duplex, and the pin signals to MDI/MDI-X (i.e., allowing these ports to be connected to any network device with straight-through cable). These ports can be connected directly to a PC or to a server equipped with an Ethernet network interface card, or to a networking device such as an Ethernet hub or switch.
- One RJ-45 port for connection to a DSL or cable modem (WAN). This port also auto-negotiates operating speed to 10/100 Mbps, the mode to half/full duplex, and the pin signals to MDI/MDI-X.

The following figure shows the components of the Wireless Barricade:

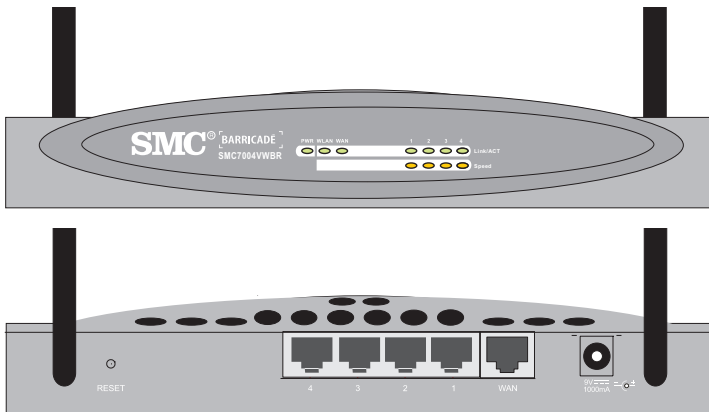


Figure 1. Front and Rear Panels

Installing the Wireless Barricade Router

Item	Description
Reset Button	Use this button to reset the power and restore the default factory settings.
LAN Ports	Fast Ethernet ports (RJ-45). Connect devices (such as a PC, hub or switch) on your local area network to these ports.
WAN Port	WAN port (RJ-45). Connect your cable modem, DSL modem, or an Ethernet router to this port.
Power Inlet	Connect the included power adapter to this inlet. Warning: Using the wrong type of power adapter may cause damage.
LEDs	Power, WAN and LAN port status indicators. (See "LED Indicators" on page 1.)

System Requirements

You must have an ISP that meets the following minimum requirements:

- Internet access from your local telephone company or Internet Service Provider (ISP) using a DSL modem or cable modem.
- A PC using a fixed IP address or dynamic IP address assigned via DHCP, as well as a gateway server address and DNS server address from your service provider.
- A computer equipped with a 10 Mbps, 100 Mbps, or 10/100 Mbps Fast Ethernet card, or a USB-to-Ethernet converter.
- TCP/IP network protocol installed on each PC that needs to access the Internet.
- A Java-enabled Web browser, such as Microsoft Internet Explorer 5.0 or above, or Netscape Communicator 4.0 or above installed on one PC at your site for configuring the Wireless Barricade.

Connect the System

The Wireless Barricade can be positioned at any convenient location in your office or home. No special wiring or cooling requirements are needed. You should, however comply with the following guidelines:

- Keep the Wireless Barricade away from any heating devices.
- Do not place the Wireless Barricade in a dusty or wet environment.

You should also remember to turn off the power, remove the power cord from the outlet, and keep your hands dry when you install the Wireless Barricade.

Basic Installation Procedure

1. Connect the LAN: You can connect the Wireless Barricade to your PC, or to a hub or switch. Run Ethernet cable from one of the LAN ports on the front of the Wireless Barricade to your computer's network adapter or to another network device.

You may also connect the Wireless Barricade to your PC (using a wireless client adapter) via radio signals. Position both antennas on the back of the Wireless Barricade into the desired positions. For more effective coverage, position one antenna along the vertical axis and the other antenna along the horizontal axis. **(The antennas emit signals along the toroidal plane – and thus provide more effective coverage when positioned along alternate axes.)**

2. Connect the WAN: Prepare an Ethernet cable for connecting the Wireless Barricade to a cable/DSL modem or Ethernet router. Prepare a serial cable for connecting the Wireless Barricade to an ISDN TA or PSTN modem.

Installing the Wireless Barricade Router

3. Power on: Connect the power adapter to the Wireless Barricade.

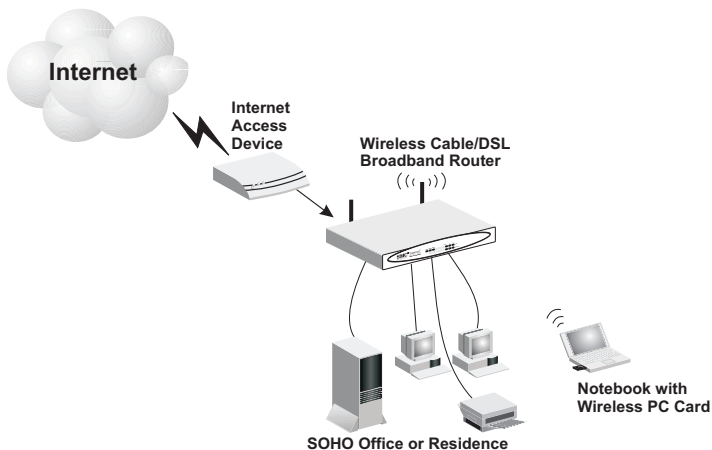


Figure 2. Connecting the Wireless Barricade Router

Attach to Your Network Using Ethernet Cabling

The four LAN ports on the Wireless Barricade auto-negotiate the connection speed to 10 Mbps Ethernet or 100 Mbps Fast Ethernet, and the transmission mode to half duplex or full duplex.

Use twisted-pair cable to connect any of the four LAN ports on the Wireless Barricade to an Ethernet adapter on your PC. Otherwise, you can cascade any of the LAN ports on the Wireless Barricade to an Ethernet hub or switch, and then connect your PC or other network equipment to the hub or switch. When inserting an RJ-45 plug, be sure the tab on the plug clicks into position to ensure that it is properly seated.

Warning: Do not plug a phone jack connector into any RJ-45 port. This may damage the Wireless Barricade. Instead, use only twisted-pair cables with RJ-45 connectors that conform with FCC standards.

Attach to Your Network Using Radio Signals

Install a wireless network adapter in each computer that will be connected to the Internet or your local network via radio signals. SMC currently offers several wireless network cards, including the SMC2602W and SMC2632W Wireless cards.

Rotate both antennas on the back of the Wireless Barricade to the desired position. For more effective coverage, position one antenna along the vertical axis and the other along the horizontal axis. Try to place the Wireless Barricade in a position that is located in the center of your wireless network. Normally, the higher you place the antenna, the better the performance. Ensure that the Wireless Barricade's location provides optimal reception throughout your home or office.

Computers equipped with a wireless adapter can communicate with each other as an independent wireless LAN by configuring each computer to the same radio channel. However, the Wireless Barricade can provide access to your wired/wireless LAN or to the Internet for all wireless workstations. Each wireless PC in this network infrastructure can talk to any computer in the wireless group via a radio link, or access other computers or network resources in the wired LAN infrastructure or over the Internet via the Wireless Barricade.

The wireless infrastructure configuration not only extends the accessibility of wireless PCs to the wired LAN, but also doubles the effective wireless transmission range for wireless PCs by retransmitting incoming radio signals through the Wireless Barricade.

A wireless infrastructure can be used for access to a central database, or for connection between mobile workers, as shown in the following figure:

Installing the Wireless Barricade Router

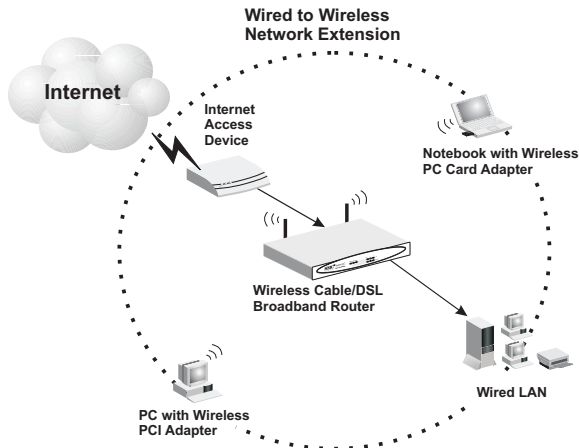


Figure 3. Making the WLAN Connections

Attach the Wireless Barricade Router to the Internet

If Internet services are provided through an xDSL or cable modem, use unshielded or shielded twisted-pair Ethernet cable (Category 3 or greater) with RJ-45 plugs to connect the broadband modem directly to the WAN port on the Wireless Barricade.

Note: When connecting to the WAN port, use 100-ohm Category 3, 4, or 5 shielded or unshielded twisted-pair cable with RJ-45 connectors at both ends for all connections.

Connecting the Power Adapter

Plug the power adapter into the power socket on the Wireless Barricade, and the other end into a power outlet. Check the indicator marked "PWR" on the front panel to be sure it is on. If the power indicator does not light, refer to "Troubleshooting" on page 65.

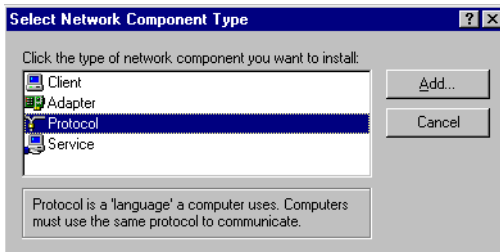
CONFIGURING CLIENT TCP/IP

If you have not previously installed the TCP/IP protocols on your client PCs, refer to the following section. If you need information on how to configure a TCP/IP address on a PC, refer to “Setting Up TCP/IP” on page 13.

Installing TCP/IP

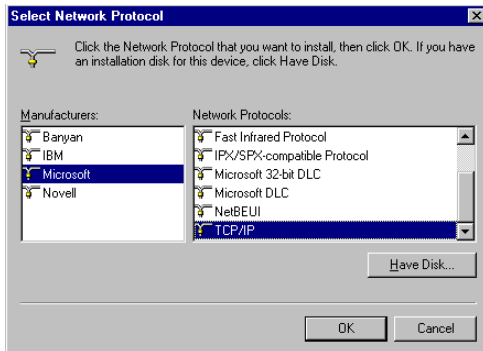
Windows 95/98/Me

1. Click Start/Settings/Control Panel.
2. Double-click the Network icon and select the Configuration tab in the Network window.
3. Click the Add button.
4. Double-click Protocol.



Configuring Client TCP/IP

5. Select Microsoft in the manufacturers list. Select TCP/IP in the Network Protocols list. Click the OK button to return to the Network window.

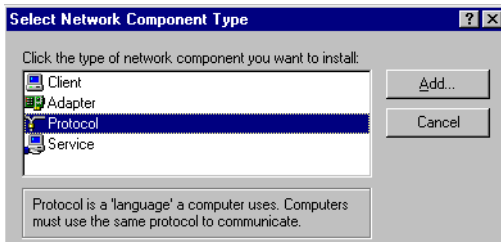


6. The TCP/IP protocol will be listed in the Network window. Click OK. The operating system may prompt you to restart your system. Click Yes and the computer will shut down and restart.

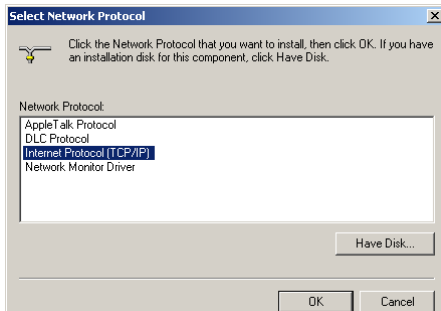
Windows 2000

1. Click the Start button and choose Settings, then click the Network and Dial-up Connections icon.
2. Double-click the Local Area Connection icon, and click the Properties button on the General tab.
3. Click the install... button.

4. Double-click Protocol.



5. Choose Internet Protocol (TCP/IP). Click the OK button to return to the Network window.



6. The TCP/IP protocol will be listed in the Network window. Click OK to complete the installation procedure.

Setting Up TCP/IP

To access the Internet through the Wireless Barricade, you must configure the network settings of the computers on your LAN to use the same IP subnet as the Wireless Barricade. The default network settings for the Wireless Barricade are:

Gateway IP Address: 192.168.2.1
Subnet Mask: 255.255.255.0

Configuring Client TCP/IP

Note: These settings may be changed to suit your network requirements, but you must first configure at least one computer as described in this chapter to access the Wireless Barricade's Web configuration interface. See "Configuring the Wireless Barricade Router" on page 25 for information on configuring the Wireless Barricade.)

If you have not previously configured TCP/IP for your computer, refer to "Configuring Client TCP/IP" on page 11. The IP address of the connected client PC should be 192.168.2.x (where x means 2–254). You can set the IP address for client PCs either by automatically obtaining an IP address from the Wireless Barricade's DHCP service or by manual configuration.

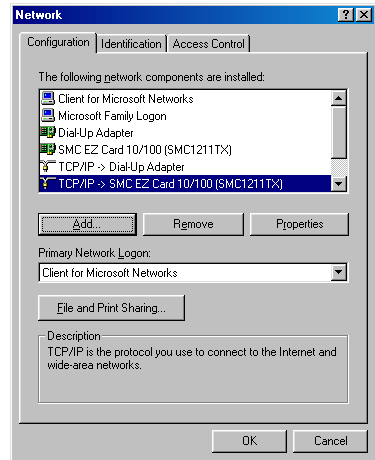
Configuring Your Computer in Windows 95/98/Me

You may find that the instructions here do not exactly match your version of Windows. This is because these steps and screenshots were created in Windows 98. Windows 95 and Windows Millennium Edition are very similar, but not identical, to Windows 98.

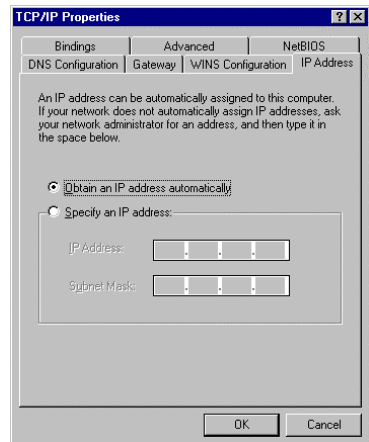
1. From the Windows desktop, click Start/Settings/Control Panel.
2. In the Control Panel, locate and double click the Network icon.

Setting Up TCP/IP

3. On the Network window Configuration tab, double-click the TCP/IP entry for your network card.



4. Click the IP Address tab.



5. Click the “Obtain an IP address” option.
6. Next click on the Gateway tab and verify the Gateway field is blank. If there are IP addresses listed in the Gateway section, highlight each one and click Remove until the section is empty.
7. Click the OK button to close the TCP/IP Properties window.

Configuring Client TCP/IP

8. On the Network Properties Window, click the OK button to save these new settings.

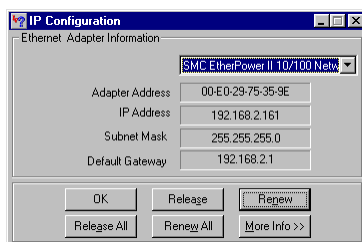
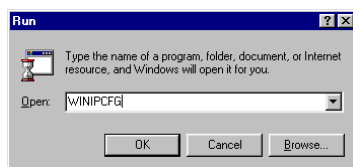
Note: Windows may ask you for the original Windows installation disk or additional files. Check for the files at c:\windows\options\cabs, or insert your Windows CD-ROM into your CDROM drive and check the correct file location, e.g., D:\win98, D:\win9x. (if D is the letter of your CD-ROM drive).

9. Windows may prompt you to restart the PC. If so, click the Yes button. If Windows does not prompt you to restart your computer, do so to insure your settings.

Obtain IP Settings from Your Wireless Barricade Router

Now that you have configured your computer to connect to your Router, it needs to obtain new network settings. By releasing old IP settings and renewing them with settings from the Wireless Barricade, you will also verify that you have configured your computer correctly.

1. Click Start/Run.
2. Type WINIPCFG and click OK.
3. From the drop-down menu, select your network card. Click Release and then Renew. Verify that your IP address is now 192.168.2.xxx, your Subnet Mask is 255.255.255.0 and your Default Gateway is 192.168. 2.1. These values confirm that the Wireless

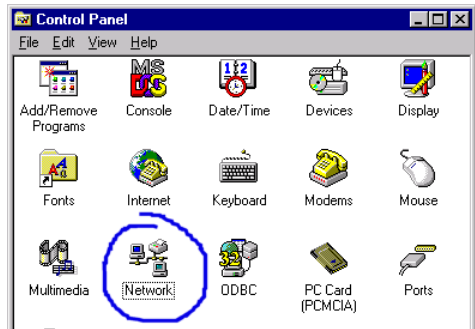


Setting Up TCP/IP

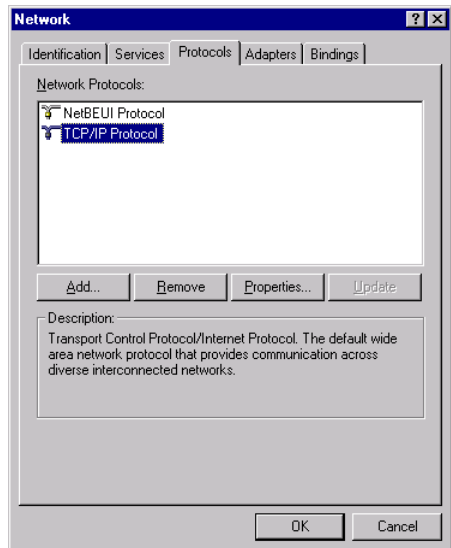
Barricade is functioning. Click OK to close the IP Configuration window.

Configuring Your Computer in Windows NT 4.0

1. From the Windows desktop click Start/Settings/Control Panel.
2. Double-click the Network icon.



3. Click on the Protocols tab.
4. Double-click TCP/IP Protocol.



5. Click on the IP Address tab.

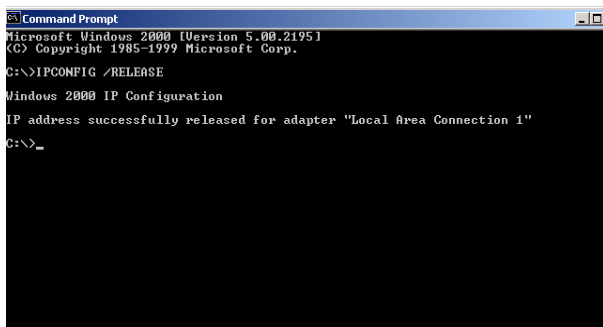
Configuring Client TCP/IP

6. In the Adapter drop-down list, be sure your Ethernet adapter is selected.
7. Click on "Obtain an IP address from a DHCP server".
8. Click OK to close the window.
9. Windows may copy files and will then prompt you to restart your system. Click Yes and your computer will shut down and restart.

Obtain IP Settings From Your Wireless Barricade Router

Now that you have configured your computer to connect to the Wireless Barricade, it needs to obtain new network settings. By releasing old IP settings and renewing them with settings from the Wireless Barricade, you will also verify that you have configured your computer correctly.

1. On the Windows desktop, click Start/Programs/Command Prompt.
2. In the Command Prompt window, type IPCONFIG /RELEASE and press the <ENTER> key.



```
Command Prompt
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

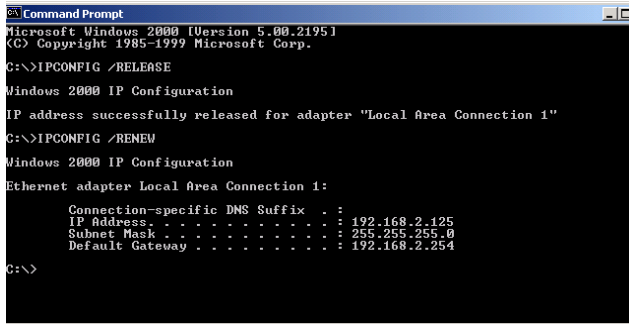
C:\>IPCONFIG /RELEASE

Windows 2000 IP Configuration

IP address successfully released for adapter "Local Area Connection 1"

C:\>_
```

3. Type `IPCONFIG /RENEW` and press the <ENTER> key. Verify that your IP Address is now 192.168.2.xxx, your Subnet Mask is 255.255.255.0 and your Default Gateway is 192.168.2.1. These values confirm that the Wireless Barricade is functioning.



```
Command Prompt
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

C:\>IPCONFIG /RELEASE

Windows 2000 IP Configuration

IP address successfully released for adapter "Local Area Connection 1"

C:\>IPCONFIG /RENEW

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection 1:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 192.168.2.125
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.2.254

C:\>
```

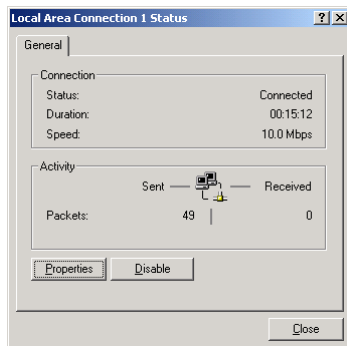
4. Type `EXIT` and press <ENTER> to close the Command Prompt window.

Configuring Your Computer in Windows 2000

1. Access your Network settings by clicking Start, then choose Settings and then select Control Panel.
2. In the Control Panel, locate and double-click the Network and Dial-up Connections icon.

Configuring Client TCP/IP

3. Locate and double-click the Local Area Connection icon for the Ethernet adapter that is connected to the Wireless Barricade. When the Status dialog box window opens, click the Properties button.
4. In the Local Area Connection Properties box, verify the box next to Internet Protocol (TCP/IP) is checked. Then highlight the Internet Protocol (TCP/IP), and click the Properties button.
5. Select “Obtain an IP address automatically” to configure your computer for DHCP. Click the [OK] button to save this change and close the Properties window.
6. Click the OK button again to save these new changes.
7. Reboot your PC.
8. To obtain new network settings see “Obtain IP Settings from Your Wireless Barricade Router” on page 16.



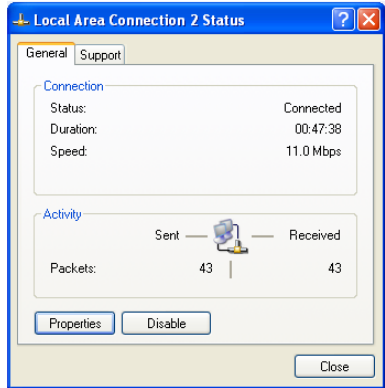
Configuring Your Computer in Windows XP

The following instructions assume you are running Windows XP with the default interface. If you are using the Classic interface (where the icons and menus look like previous Windows versions), please follow the instructions for Windows 2000 outlined above.

1. Access your Network settings by clicking Start, choose Control Panel, select Network and Internet Connections and then click on the Network Connections icon.

Setting Up TCP/IP

2. Locate and double-click the Local Area Connection icon for the Ethernet adapter that is connected to the Wireless Barricade. Next, click the Properties button.



3. In the Local Area Connection Properties box, verify the box next to Internet Protocol (TCP/IP) is checked. Then highlight the Internet Protocol (TCP/IP), and click the Properties button.
4. Select "Obtain an IP address automatically" to configure your computer for DHCP. Click the OK button to save this change and close the Properties window.
5. Click the OK button again to save these new changes.
6. Reboot your PC.

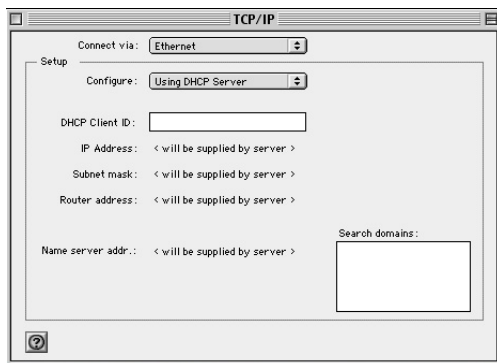
Configuring a Macintosh Computer

You may find that the instructions here do not exactly match your screen. This is because these steps and screenshots were created using Mac OS 8.5. Mac OS 7.x and above are all very similar, but may not be identical to Mac OS 8.5.

1. Pull down the Apple Menu. Click Control Panel and select TCP/IP.

Configuring Client TCP/IP

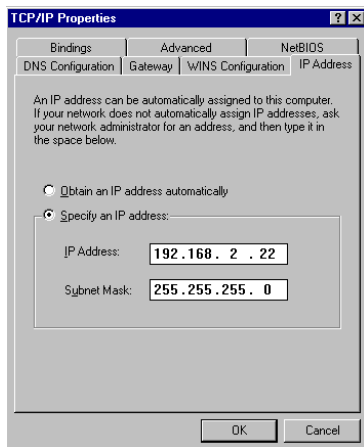
2. In the TCP/IP dialog box, make sure that Ethernet is selected in the Connect Via: field.
3. Select Using DHCP Server in the Configure field.



4. Close the TCP/IP dialog box.

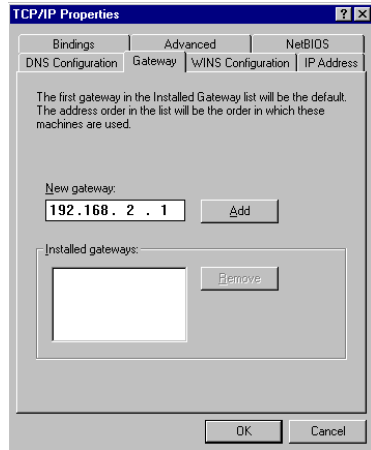
Manual IP Configuration

1. Check Specify an IP address on the IP Address tab. Enter an IP address based on the default network 192.168.2.x (where x is between 2 and 254), and use 255.255.255.0 for the subnet mask.

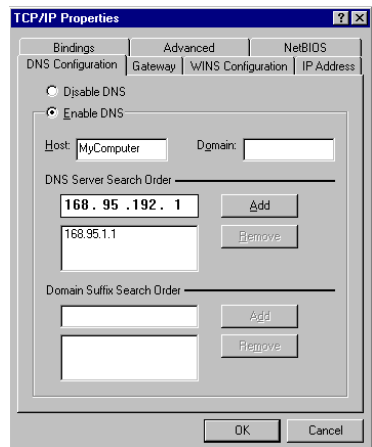


Setting Up TCP/IP

2. In the Gateway tab, add the IP address of the Wireless Barricade (default: 192.168.2.1) in the New gateway field and click Add.



3. On the DNS Configuration tab, add the IP address for the Wireless Barricade and click Add. This automatically relays DNS requests to the DNS server(s) provided by your ISP. Otherwise, add specific DNS servers into the DNS Server Search Order field and click Add.



4. After finishing TCP/IP setup, click OK, and then reboot the computer. After that, set up other PCs on the LAN according to the procedures described above.

Verifying Your TCP/IP Connection

After installing the TCP/IP communication protocols and configuring an IP address in the same network as the Wireless Barricade, use the Ping command to check if your computer has successfully connected to the Wireless Barricade. The following example shows how the Ping procedure can be executed in an MS-DOS window. First, execute the Ping command:

```
ping 192.168.2.1
```

If a message similar to the following appears:

```
Pinging 192.168.2.1 with 32 bytes of data:  
Reply from 192.168.2.1: bytes=32 time=2ms TTL=64
```

a communication link between your computer and the Wireless Barricade has been successfully established.

If you get the following message,

```
Pinging 192.168.2.1 with 32 bytes of data:  
Request timed out.
```

there may be something wrong in your installation procedure. Check the following items in sequence:

1. Is the Ethernet cable correctly connected between the Wireless Barricade and the computer?

The LAN LED on the Wireless Barricade and the Link LED of the network card on your computer must be on.

2. Is TCP/IP properly configured on your computer?

If the IP address of the Wireless Barricade is 192.168.2.1, the IP address of your PC must be from 192.168.2.2 - 192.168.2.254 and the default gateway must be 192.168.2.1.

If you can successfully Ping the Wireless Barricade you are now ready to connect to the Internet!

CONFIGURING THE WIRELESS BARRICADE ROUTER

The Wireless Barricade Router can be configured by any Java-supported browser including Internet Explorer 5.0 or above, or Netscape Navigator 4.0 or above. Using the Web management interface, you can configure the Wireless Barricade and view statistics to monitor network activity.

Note: Before you attempt to configure your router, if you have access to the Internet please visit www.smc.com and download the latest firmware update to insure your router is running the latest

Before you attempt to log into the Wireless Barricade's Web-based Administration, please verify the following.

1. Your browser is configured properly (see below).
2. Disable any firewall or security software that may be running.
3. Confirm that you have a good link LED where your computer is plugged into the Wireless Barricade. If you don't have a link light – then try another cable until you get a good link.

Browser Configuration

Confirm your browser is configured for a direct connection to the Internet using the Ethernet cable that is installed in the computer. This is configured through the options/preference section of your browser.

Disable Proxy Connection

You will also need to verify that the HTTP Proxy feature of your web browser is disabled. This is so that your web browser will be able to view the Wireless Barricade configuration pages. The following steps are for Internet Explorer and for Netscape.

Determine which browser you use and follow the appropriate steps.

Internet Explorer (5 or above)

1. Open Internet Explorer. Click Tools, and then select Internet Options.
2. In the Internet Options window, click the Connections tab.
3. Click the LAN Settings button.
4. Clear all the check boxes and click OK to save these LAN settings changes.
5. Click OK again to close the Internet Options window.

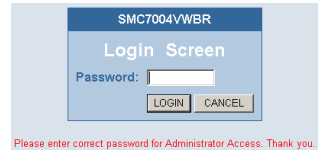
Internet Explorer (For Macintosh)

1. Open Internet Explorer. Click Edit/Preferences.
2. In the Internet Explorer Preferences window, under Network, select Proxies.
3. Uncheck all checkboxes and click OK.

Netscape (4 or above)

1. Open Netscape. Click Edit, and then select Preferences.
2. In the Preferences window, under Category, double-click Advanced, then select the Proxies option.
3. Check “Direct connection to the Internet.”
4. Click the OK button to save the changes.

To access the Wireless Barricade’s management interface, enter the Wireless Barricade IP address in your Web browser <http://192.168.2.1>. Then click LOGIN. (By default, there is no password.)



The home page displays the Setup Wizard and Advanced Setup options.



Navigating the Web Browser Interface

The Wireless Barricade's management interface features a Setup Wizard and an Advanced Setup section. Use the Setup Wizard if you want to quickly set up the Wireless Barricade for use with a cable modem or DSL modem.

Advanced setup supports more advanced functions like hacker attack detection, IP and MAC address filtering, intrusion detection, virtual server setup, virtual DMZ hosts, and other advanced functions.

Making Configuration Changes

Configurable parameters have a dialog box or a drop-down list. Once a configuration change has been made on a page, be sure to click the APPLY or NEXT button at the bottom of the page to enable the new setting.

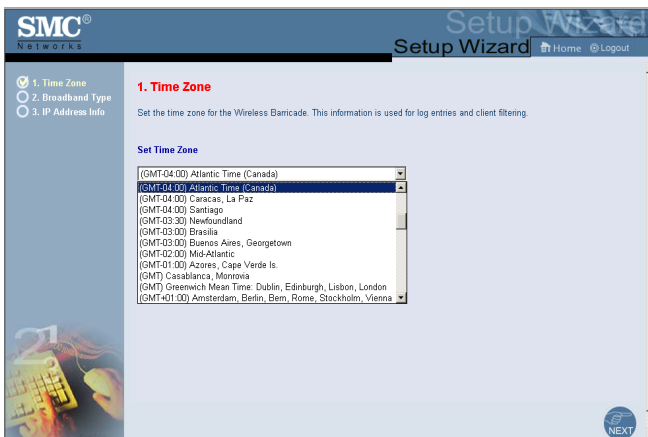
Note: To ensure proper screen refresh after a command entry, ensure that Internet Explorer 5.0 is configured as follows: Under the menu Tools/Internet Options/General/Temporary Internet Files/Settings, the setting for "Check for newer versions of stored pages" should be "Every visit to the page."

Setup Wizard

Time Zone

Click on the Setup Wizard picture. The first item in the Setup Wizard is Time Zone setup.

For accurate timing of client filtering and log events, you need to set the time zone. Select your time zone from the drop-down list, and click NEXT.



Broadband Type

Select the type of broadband connection you have.

For a cable modem connection see the following page. For a Fixed-IP xDSL connection see “Fixed-IP xDSL” on page 31, for a PPPoE xDSL connection, see “PPPoE xDSL” on page 31, and for BigPond connection, see “BigPond” on page 33.

Configuring the Wireless Barricade Router



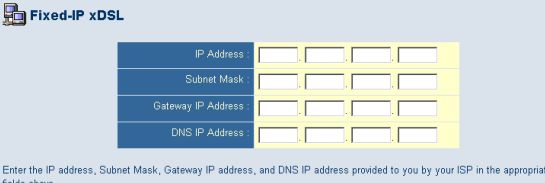
Cable Modem

The screenshot shows the 'Cable Modem' configuration screen. It has a light blue background. At the top left, there's a 'Cable Modem' icon and label. Below it, there's a 'Host Name' field with a text input box. Underneath that is a 'MAC Address' field with a table of input boxes. The table has five rows and five columns. The first row contains '00', '04', 'c2', '7a', and '25'. The second row contains '25' and '25'. Below the table is a 'Clone MAC Address' button. At the bottom, there's a small note: 'A cable modem requires minimal configuration. If the ISP requires you to input a Host Name, type it in the "Host Name" field above.'

Your ISP may have given you a host name. If so, enter it into the field.

Click Finish to complete the setup. The Status page will open to allow you to view the connection status, as well as other information. See “Status” on page 64 for details.

Fixed-IP xDSL



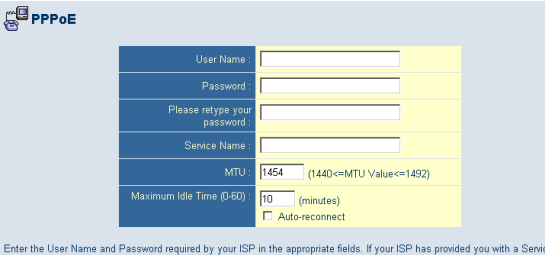
Fixed-IP xDSL

IP Address	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Subnet Mask	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Gateway IP Address	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
DNS IP Address	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Enter the IP address, Subnet Mask, Gateway IP address, and DNS IP address provided to you by your ISP in the appropriate fields above.

Some xDSL Internet Service Providers may assign a fixed (static) IP address. If you have been provided with this information, choose this option and enter the assigned IP address, gateway IP address, DNS IP addresses, and subnet mask. Click FINISH to complete the setup.

PPPoE xDSL



PPPoE

User Name	<input type="text"/>
Password	<input type="password"/>
Please retype your password	<input type="password"/>
Service Name	<input type="text"/>
MTU	1454 (1440 <= MTU Value <= 1492)
Maximum Idle Time (0-60)	10 (minutes)
	<input type="checkbox"/> Auto-reconnect

Enter the User Name and Password required by your ISP in the appropriate fields. If your ISP has provided you with a Service Name enter it in the "Service Name" field, otherwise, leave it blank.

Enter the PPPoE User Name and Password assigned by your Service Provider. The Service Name is normally optional, but may be required by some service providers.

Leave the Maximum Transmission Unit (MTU) at the default value (1454) unless you have a particular reason to change it.

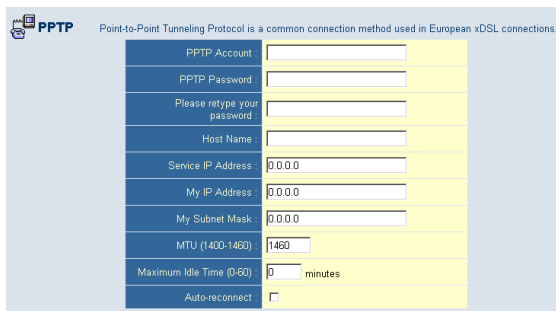
Enter a Maximum Idle Time (in minutes) to define a maximum period of time for which the Internet connection is maintained

Configuring the Wireless Barricade Router

during inactivity. If the connection is inactive for longer than the Maximum Idle Time, it will be dropped. (Default: 10)

Enable the Auto-reconnect option to automatically re-establish the connection as soon as you attempt to access the Internet again. Click FINISH to complete the setup.

PPTP (Point-to-Point Tunneling Protocol)



Point-to-Point Tunneling Protocol is a common connection method used in European xDSL connections.

PPTP Account:	<input type="text"/>
PPTP Password:	<input type="password"/>
Please retype your password:	<input type="password"/>
Host Name:	<input type="text"/>
Service IP Address:	<input type="text" value="0.0.0.0"/>
My IP Address:	<input type="text" value="0.0.0.0"/>
My Subnet Mask:	<input type="text" value="0.0.0.0"/>
MTU (1400-1460):	<input type="text" value="1460"/>
Maximum Idle Time (0-60):	<input type="text" value="0"/> minutes
Auto-reconnect:	<input type="checkbox"/>

Point-to-Point Tunneling Protocol is a common connection method used for xDSL connections in Europe. It can be used to join different physical networks using the Internet as an intermediary.

If you have been provided with the information as shown on the screen, enter the assigned IP address, subnet mask, default gateway IP address, user ID and password, and PPTP Gateway.

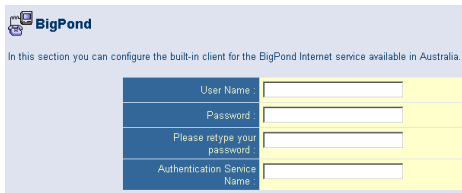
The MTU (Maximum Transmission Unit) governs the maximum size of the data packets. Leave this on the default value (1460) unless you have a particular reason to change it.

Enter a Maximum Idle Time (in minutes) to define a maximum period of time for which the Internet connection is maintained during inactivity. If the connection is inactive for longer than the Maximum Idle Time, it will be dropped. (Default: 0)

Enable the Auto-reconnect option to automatically re-establish the connection as soon as you attempt to access the Internet again.

Click FINISH to complete the setup. (Refer to “Point-to-Point Tunneling Protocol (PPTP)” on page 40 for details.)

BigPond

The image shows a software window titled "BigPond" with a small icon of a computer and a globe. Below the title bar, a line of text reads: "In this section you can configure the built-in client for the BigPond Internet service available in Australia." Below this text is a form with four rows, each with a label on the left and a text input field on the right. The labels are: "User Name:", "Password:", "Please retype your password:", and "Authentication Service Name:". The input fields are empty and have a yellow background. The form is set against a light blue background.

User Name :	<input type="text"/>
Password :	<input type="password"/>
Please retype your password :	<input type="password"/>
Authentication Service Name :	<input type="text"/>

If you use the BigPond Internet Service which is available in Australia, enter the the user name, password and service name for BigPond authentication. Click FINISH to complete the setup.

Advanced Setup

Use the Web management interface to define system parameters, manage and control the Wireless Barricade and its ports, or monitor network conditions. The following table outlines the selections available from this program.

Menu	Description
System	Sets the local time zone, the password for administrator access, and the IP address of a PC that will be allowed to manage the Wireless Barricade remotely.
WAN	Specifies the Internet connection type: <ul style="list-style-type: none">• Dynamic IP host configuration and the physical MAC address of each media interface• PPPoE configuration• PPTP• Static IP and ISP gateway address• BigPond (Internet service available in Australia)• Specifies DNS servers to use for domain name resolution.
LAN	Sets the TCP/IP configuration of the Wireless Barricade's LAN interface and all DHCP clients.
Wireless	Configures the radio frequency, SSID, and encryption for wireless communications.
NAT	Shares a single ISP account with multiple users, sets up virtual servers.
Firewall	Configures a variety of security and specialized functions, including: Access Control, Hacker Prevention, and DMZ.
DDNS	Dynamic DNS provides users on the Internet with a method to tie their domain name(s) to computers or servers.
UPnP	With Universal Plug and Play, a device can automatically dynamically join a network, obtain an IP address, communicate its capabilities, and learn about the presence and capabilities of other devices. Devices can then directly communicate with each other. This further enables peer to peer networking.
Tools	Contains options to backup & restore the current configuration, restore all configuration settings to the factory defaults, update system firmware, or reset the system.

Menu	Description
Status	<p>Provides WAN connection type and status, firmware and hardware version numbers, system IP settings, as well as DHCP, NAT, and Firewall information.</p> <p>Displays the number of attached clients, the firmware versions, the physical MAC address for each media interface, and the hardware version and serial number.</p> <p>Shows the security and DHCP client log.</p>

System

Time Zone

SMC® Networks Advanced Setup [Home](#) [Logout](#)

- System
 - Time Zone
 - Password Settings
 - Remote Management
- WAN
- LAN
- Wireless
- NAT
- Firewall
- DDNS
- UPnP
- Tools
- Status

Time Zone

Set the time zone of the Wireless Barricade. This information is used for log entries and client filtering.

Set Time Zone
 (GMT-04:00) Atlantic Time (Canada)

Configure Time Server (NTP):
 You can automatically maintain the system time on your SMC Barricade by synchronizing with a public time server over the Internet.

☒ Enable Automatic Time Server Maintenance

When you enable this option you will need to configure two different time servers, use the options below to set the primary and secondary NTP servers in your area.

Primary Server: 132.163.4.102 - North America

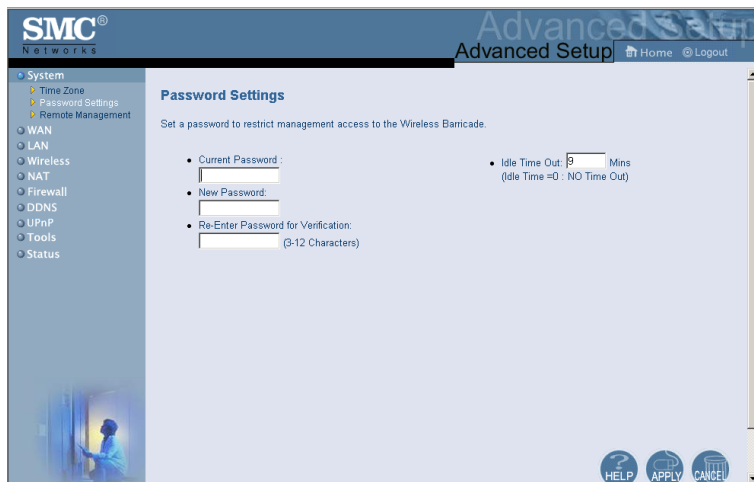
Secondary Server: 192.5.41.41 - North America

[HELP](#) [APPLY](#) [CANCEL](#)

Select your time zone and time server from the drop-down list for the Wireless Barricade. This information is used for log entries and client access control.

Configuring the Wireless Barricade Router

Password Settings



The screenshot shows the SMC Networks Advanced Setup web interface. The left sidebar contains a navigation menu with the following items: System (selected), Time Zone, Password Settings, Remote Management, WAN, LAN, Wireless, NAT, Firewall, DDNS, UPnP, Tools, and Status. The main content area is titled "Password Settings" and includes the instruction: "Set a password to restrict management access to the Wireless Barricade." Below this instruction are three configuration fields: "Current Password:" with a text input field, "New Password:" with a text input field, and "Re-Enter Password for Verification:" with a text input field and a "(3-12 Characters)" label. To the right of the "Current Password:" field is an "Idle Time Out:" section with a numeric input field set to "9" and a "Mins" label, with a note "(Idle Time =0 : NO Time Out)". At the bottom right of the interface are three circular buttons labeled "HELP", "APPLY", and "CANCEL".

Use this menu to restrict access based on a password. By default, there is no password. For security you should assign one before exposing the Wireless Barricade to the Internet.

Passwords can contain from 3–12 alphanumeric characters and are not case sensitive.

Note: If your password is lost, or you cannot gain access to the user interface, press the Reset button on the front panel (holding it down for at least five seconds) to restore the factory defaults. (The default is no password.)

Enter a maximum Idle Time Out (in minutes) to define a maximum period of time for which the login session is maintained during inactivity. If the connection is inactive for longer than the maximum idle time, it will perform system logout, and you have to login to the Web management system again.
(Default: 9 minutes)

Remote Management

The screenshot shows the SMC Networks Advanced Setup web interface. On the left is a navigation menu with categories: System (Time Zone, Password Settings, Remote Management), WAN, LAN, Wireless, NAT, Firewall, DDNS, UPnP, Tools, and Status. The 'Remote Management' option under System is highlighted. The main content area is titled 'Remote Management' and contains the following text: 'Set the remote management of the Wireless Barricade. If you want to manage the Wireless Barricade from a remote location (outside of the local network), you must also specify the IP address of the remote PC.' Below this text is a table with two columns: 'Host Address' and 'Enabled'. The 'Host Address' column contains four input fields, each with a '0' entered. The 'Enabled' column contains a checkbox that is currently unchecked. At the bottom right of the interface are three circular buttons: 'HELP', 'APPLY', and 'CANCEL'.

Host Address	Enabled
0 0 0 0	<input type="checkbox"/>

Remote Management allows a remote PC to configure, manage, and monitor the Wireless Barricade using a standard Web browser. Check Enable and enter the IP address of the remote host. Click APPLY.

Note: If you specify 0.0.0.0 as this IP address, any host can manage the Wireless Barricade.

WAN

Specify the WAN connection type provided by your Internet Service Provider, then click More Configuration to enter detailed configuration parameters for the selected connection type.

Configuring the Wireless Barricade Router

Dynamic IP

The screenshot shows the SMC Networks Advanced Setup interface. On the left is a navigation menu with categories: System, WAN, LAN, Wireless, NAT, Firewall, DDNS, UPnP, Tools, and Status. Under the WAN category, the following options are listed: Dynamic IP (selected), PPPoE, PPTP, Static IP, BigPond, and DNS. The main content area is titled 'Dynamic IP' and contains the following text: 'The Host name is optional, but may be required by some Service Provider's. The default MAC address is set to the WAN's physical interface on the Wireless Barricade.' Below this, it states: 'If required by your Service Provider, you use the "Clone MAC Address" button to copy the MAC address of the Network Interface Card installed in your PC to replace the WAN MAC address.' Further down, it says: 'If necessary, you can use the "Release" and "Renew" buttons on the Status page to release and renew the WAN IP address.'

The configuration fields are as follows:

Host Name :	<input type="text"/>
MAC Address :	<input type="text" value="00"/> <input type="text" value="34"/> <input type="text" value="e2"/> <input type="text" value="7a"/> <input type="text" value="25"/> <input type="text" value="45"/>
	<input type="button" value="Clone MAC Address"/>

At the bottom right of the page are three circular buttons: HELP, APPLY, and CANCEL.

The Host Name is optional, but may be required by some ISPs. The default MAC address is set to the WAN's physical interface on the Wireless Barricade. Use this address when registering for Internet service, and do not change it unless required by your ISP. If your ISP used the MAC address of an Ethernet card as an identifier when first setting up your broadband account, only connect the PC with the registered MAC address to the Wireless Barricade and click the Clone MAC Address button. This will replace the current Router MAC address with the already registered Ethernet card MAC address.

If you are unsure of which PC was originally set up by the broadband technician, call your ISP and request that they register a new MAC address for your account. Register the default MAC address of the Wireless Barricade.

Point-to-Point Over Ethernet (PPPoE)

The screenshot shows the SMC Networks Advanced Setup window. On the left is a navigation tree with categories: System, WAN, LAN, Wireless, NAT, Firewall, DDNS, UPnP, Tools, and Status. The WAN category is expanded, showing sub-options: Dynamic IP, PPP, Static IP, BigPond, and DNS. The PPP option is selected. The main content area is titled 'PPPoE' and contains a descriptive paragraph about entering user name and password. Below the text is a form with the following fields: 'User Name' (text input), 'Password' (password input), 'Please retype your password' (password input), 'Service Name' (text input), 'MTU' (numeric input with a default of 1454 and a range constraint '(1440<=MTU Value<=1492)'), 'Maximum Idle Time (0-140):' (numeric input with a default of 10 and a unit of '(minutes)'), and an 'Auto-reconnect' checkbox. At the bottom right of the window are three buttons: 'HELP', 'APPLY', and 'CANCEL'.

SMC®
Networks

Advanced Setup Home Logout

System
WAN
 Dynamic IP
 PPP
 Static IP
 BigPond
 DNS
LAN
Wireless
NAT
Firewall
DDNS
UPnP
Tools
Status

PPPoE

Enter the PPPoE user name and password assigned by your Service Provider. The Service Name is normally optional, but may be required by some service providers. Enter a Maximum Idle Time (in minutes) to define a maximum period of time for which the Internet connection is maintained during inactivity. If the connection is inactive for longer than the Maximum Idle Time, then it will be dropped. You can enable the Auto-reconnect option to automatically re-establish the connection as soon as you attempt to access the Internet again. If your Internet Service Provider requires the use of PPPoE, enter the information below.

User Name

Password

Please retype your password

Service Name

MTU (1440<=MTU Value<=1492)

Maximum Idle Time (0-140): (minutes)

☐ Auto-reconnect

HELP APPLY CANCEL

Enter the PPPoE User Name and Password assigned by your Service Provider. The Service Name is normally optional, but may be required by some service providers.

The MTU (Maximum Transmission Unit) governs the maximum size of the data packets. Leave this on the default value (1454) unless you have a particular reason to change it.

Enter a Maximum Idle Time (in minutes) to define a maximum period of time for which the Internet connection is maintained during inactivity. If the connection is inactive for longer than the Maximum Idle Time, it will be dropped. (Default: 10 minutes)

Enable the Auto-reconnect option to automatically re-establish the connection as soon as you attempt to access the Internet again.

Configuring the Wireless Barricade Router

Point-to-Point Tunneling Protocol (PPTP)

The screenshot shows the SMC Networks Advanced Setup web interface. On the left is a navigation menu with categories: System, WAN, LAN, Wireless, NAT, Firewall, DDNS, UPnP, Tools, and Status. The WAN category is expanded, showing sub-items: Dynamic IP, PPPoE, PPTP (selected), Static IP, BigPond, and DNS. The main content area is titled 'PPTP' and includes a descriptive text: 'Point-to-Point Tunneling Protocol is a common connection method used in European xDSL connections.' Below this is a configuration table with the following fields:

PPTP Account	<input type="text"/>
PPTP Password	<input type="password"/>
Please retype your password	<input type="password"/>
Host Name	<input type="text"/>
Service IP Address	<input type="text" value="0.0.0.0"/>
My IP Address	<input type="text" value="0.0.0.0"/>
My Subnet Mask	<input type="text" value="0.0.0.0"/>
MTU (1400-1460)	<input type="text" value="1460"/>
Maximum Idle Time (0-60)	<input type="text" value="0"/> minutes
Auto-reconnect	<input type="checkbox"/>

At the bottom right of the interface are three buttons: HELP, APPLY, and CANCEL.

Point-to-Point Tunneling Protocol (PPTP) can be used to join different physical networks using the Internet as an intermediary. Using the above screen allows client PCs to establish a normal PPTP session and provides hassle-free configuration of the PPTP client on each client PC.

Enter the assigned IP address, subnet mask and default gateway IP address (usually supplied by your ISP), and then the PPTP User ID, Password and PPPTP Gateway IP address.

The MTU (Maximum Transmission Unit) governs the maximum size of the data packets. Leave this on the default value (1460) unless you have a particular reason to change it.

Enter a maximum Idle Time Out (in minutes) to define a maximum period of time for which the PPTP connection is maintained during inactivity. If the connection is inactive for

longer than the Maximum Idle Time, it will be dropped.
(Default: 10 minutes)

Enable the Auto-reconnect option to automatically re-establish the connection as soon as you attempt to access the Internet again.

Static IP

The screenshot shows the SMC Networks Advanced Setup interface. On the left is a navigation tree with categories: System, WAN, LAN, Wireless, NAT, Firewall, DDNS, UPnP, Tools, and Status. The WAN category is expanded, showing options like Dynamic IP, PPPoE, PPTP, Static IP (highlighted), BigPond, and DNS. The main content area is titled 'Static IP' and contains the following text: 'If your Service Provider has assigned a fixed IP address, enter the assigned IP address, subnet mask and the gateway address provided.' and 'Has your Service Provider given you an IP address and Gateway address?'. Below this text are three input fields, each with a label and a four-part numeric input box: 'IP address assigned by your Service Provider', 'Subnet Mask', and 'Service Provider Gateway Address'. At the bottom right of the main area are three buttons: HELP, APPLY, and CANCEL.

If your Internet Service Provider has assigned a fixed IP address, enter the assigned address and subnet mask for the Wireless Barricade, then enter the gateway address of your ISP.

You may need a fixed address if you want to provide Internet services, such as a Web server or FTP server.

Configuring the Wireless Barricade Router

BigPond

The screenshot shows the 'Advanced Setup' interface for an SMC Networks router. On the left is a navigation menu with categories: System, WAN, LAN, Wireless, NAT, Firewall, DDNS, UPnP, Tools, and Status. Under the 'WAN' category, options include Dynamic IP, PPPoE, PPTP, Static IP, and BigPond (which is highlighted in yellow). The main content area is titled 'BigPond' and contains the text: 'In this section you can configure the built-in client for the BigPond Internet service available in Australia.' Below this text is a form with four input fields: 'User Name', 'Password', 'Please retype your password', and 'Authentication Service Name'. Each field has a corresponding label and a yellow highlight. At the bottom right of the form area are three circular buttons: 'HELP' (with a question mark), 'APPLY' (with a checkmark), and 'CANCEL' (with an 'X').

User Name	<input type="text"/>
Password	<input type="password"/>
Please retype your password	<input type="password"/>
Authentication Service Name	<input type="text"/>

BigPond is a service provider in Australia that uses a heartbeat system to maintain the Internet connection. Configure the built-in client with your user name, password and service name to get online. Leave the Authentication Service Name as “login-server” for a universal configuration.

DNS

The screenshot shows the SMC Networks Advanced Setup interface. On the left is a navigation menu with categories: System, WAN, LAN, Wireless, NAT, Firewall, DDNS, UPnP, Tools, and Status. The WAN category is expanded, showing options like Dynamic IP, PPPoE, PPTP, Static IP, and BigPond. The main content area is titled 'DNS' and contains a descriptive paragraph about DNS servers. Below the text are two input fields: 'Domain Name Server (DNS) Address' and 'Secondary DNS Address (optional)', each with four character boxes. At the bottom right are three buttons: HELP, APPLY, and CANCEL.

SMC®
Networks

Advanced Setup Home Logout

DNS

A Domain Name Server (DNS) is an index of IP addresses and Web addresses. If you type a Web address into your browser, such as www.accton.com, a DNS server will find that name in its index and find the matching IP address: 64.147.25.20. Most ISPs provide a DNS server for speed and convenience. Since your Service Provider may connect to the Internet with dynamic IP settings, it is likely that the DNS server IP's are also provided dynamically. However, if there is a DNS server that you would rather use, you need to specify the IP address here.

Domain Name Server (DNS) Address

Secondary DNS Address (optional)

HELP APPLY CANCEL

Domain Name Servers map numerical IP addresses to the equivalent domain name (e.g., www.smc.com). Your ISP should provide the IP address of one or more domain name servers. Enter those addresses in this screen.

Configuring the Wireless Barricade Router

LAN

SMC® Networks Advanced Setup Home Logout

LAN Settings

You can enable DHCP to dynamically allocate IP addresses to your client PCs, or configure filtering functions based on specific clients or protocols. The Wireless Barricade must have an IP address for the local network.

LAN IP

IP Address: 192 168 2 1
IP Subnet Mask: 255.255.255.0
DHCP Server: ☒ Enabled ☐ Disabled
Lease Time: One week
IP Address Pool
Start IP: 192 168 2 100
End IP: 192 168 2 199
Domain Name: (optional)

HELP APPLY CANCEL

- **LAN IP** – Use the LAN menu to configure the LAN IP address for the Wireless Barricade and to enable the DHCP server for dynamic client address allocation.
- **Lease Time** - Set a period for the lease time if required. For home networks this may be set to Forever, which means there is no time limit on the IP address lease.
- **IP Address Pool** – A dynamic IP start address may be specified by the user, e.g. 192.168.2.100 (default value). Once this start IP address has been assigned, IP addresses running from 192.168.2.100 to 192.168.2.199 will be part of the dynamic IP address pool. IP addresses from 192.168.2.2 to 192.168.2.99, and 192.168.2.200 to 192.168.2.254 will be available as static IP addresses.

Remember not to include the address of the Wireless Barricade in the client address pool. Also remember to configure your client PCs for dynamic IP address allocation.

Wireless

To configure the Wireless Barricade as a wireless access point for wireless clients (either stationary or roaming), all you need to do is define the radio channel, the Service Set identifier (SSID), and encryption options.

Channel and SSID

SSID:	SMC
Transmission Rate:	Fully Automatic
Basic Rate:	2Mbps
Channel:	6
Broadcast SSID:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable

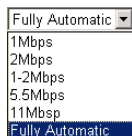
You must specify a common radio channel and SSID (Service Set ID) to be used by the Wireless Barricade and all of your wireless clients. Be sure you configure all of your clients to the same values.

ESSID: The Service Set ID. This should be set to the same value as other wireless devices in your network. (Default: SMC.)

Note: The SSID is case sensitive and can consist of up to 32 alphanumeric characters.

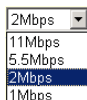
Configuring the Wireless Barricade Router

Transmission Rate: Set the data rate transmitted from the Wireless Barricade. The lower the data rate, the longer the transmission distance. (Default: Fully Automatic.)



A dropdown menu for Transmission Rate. The top option is 'Fully Automatic' with a downward arrow. Below it are '1Mbps', '2Mbps', '1-2Mbps', '5.5Mbps', and '11Mbps'. The bottom option is 'Fully Automatic' with an upward arrow.

Basic Rate: The highest rate specified is the rate the Wireless Barricade will use when transmitting broadcast/multicast and management frames. Available options are: 1, 2, 5.5, and 11Mbps. (Default: 2Mbps.)



A dropdown menu for Basic Rate. The top option is '2Mbps' with a downward arrow. Below it are '11Mbps', '5.5Mbps', '2Mbps' (highlighted), and '1Mbps'.

Channel: The radio channel through which the Wireless Barricade communicates with PCs in its BSS. (Default: 6)

Note: The available channel settings are limited by local regulations.

Broadcast SSID: Broadcasting the SSID on the wireless network for easy connection with client PCs. (Default: Enable)

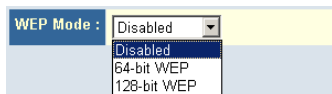


A dropdown menu for Channel. The top option is 'Auto' with a downward arrow. Below it are numbers 1 through 10. The bottom option is 'Auto' with an upward arrow.

Encryption

If you are transmitting sensitive data across wireless channels, you should enable Wired Equivalent Privacy (WEP)

encryption. Encryption requires you to use the same set of encryption/decryption keys for the Wireless Barricade and all of your wireless clients. You can choose between standard 64-bit or the more robust 128-bit encryption.



A dropdown menu for WEP Mode. The top option is 'Disabled' with a downward arrow. Below it are 'Disabled' (highlighted), '64-bit WEP', and '128-bit WEP'.

Advanced Setup

You may automatically generate encryption keys or manually enter the keys. For automatic 64-bit security, enter a passphrase and click Generate. Four keys will be generated (as shown below). Choose a key from the drop-down list or accept the default key. Automatic 128-bit security generates a single key.

SMC® Networks Advanced Setup Home Logout

System
WAN
LAN
Wireless
Channel and SSID
Encryption
NAT
Firewall
DDNS
UPnP
Tools
Status

Encryption

Encryption transmits your data securely over the wireless network. Matching encryption keys must be setup on your Wireless Barricade and wireless client devices to use encryption. Do you want to use encryption?

WEP Mode : 64-bit WEP

Enter a passphrase and click the Generate button, or manually enter a key into the table.

Passphrase :

Key 1 :	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	Default Key : 1
Key 2 :	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	
Key 3 :	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	
Key 4 :	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	

HELP APPLY CANCEL

SMC® Networks Advanced Setup Home Logout

System
WAN
LAN
Wireless
Channel and SSID
Encryption
NAT
Firewall
DDNS
UPnP
Tools
Status

Encryption

Encryption transmits your data securely over the wireless network. Matching encryption keys must be setup on your Wireless Barricade and wireless client devices to use encryption. Do you want to use encryption?

WEP Mode : 128-bit WEP

Enter a passphrase and click the Generate button, or manually enter a key into the table.

Passphrase :

Key :	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

HELP APPLY CANCEL

Configuring the Wireless Barricade Router

If you use encryption, configure the same keys used for the Wireless Barricade on each of your wireless clients. Note that Wired Equivalent Privacy (WEP) protects data transmitted between wireless nodes, but does not protect any transmissions over your wired network or over the Internet.

Network Address Translation (NAT)

From this section you can configure the Address Mapping, Virtual Server, and Special Application features that provide control over the port openings in the Wireless Barricade's firewall. This section can be used to support several Internet based applications such as VPN

Address Mapping

The screenshot shows the SMC Networks Advanced Setup web interface. The left sidebar contains a navigation menu with the following items: System, WAN, LAN, Wireless, NAT (selected), Virtual Server, Special Application, Firewall, DDNS, UPnP, Tools, and Status. The main content area is titled "Address Mapping" and includes a descriptive paragraph: "Network Address Translation (NAT) allows IP addresses used in a private local network to be mapped to one or more addresses used in the public, global Internet. This feature limits the number of public IP addresses required from the ISP and also maintains the privacy and security of the local network. We allow one or more than one public IP address to be mapped to a pool of local addresses." Below this text is a table with 6 rows for configuring address mappings. Each row has a "Global IP" field, a description "is transformed as multiple virtual IPs", and a "from" field with a range of internal IP addresses. The "Global IP" field is set to 192.168.2.0 and the "from" field is set to 192.168.2.0 for all rows.

Address Mapping	
1. Global IP: 192.168.2.0	is transformed as multiple virtual IPs
from 192.168.2.0 to 192.168.2.0	
2. Global IP: 192.168.2.0	is transformed as multiple virtual IPs
from 192.168.2.0 to 192.168.2.0	
3. Global IP: 192.168.2.0	is transformed as multiple virtual IPs
from 192.168.2.0 to 192.168.2.0	
4. Global IP: 192.168.2.0	is transformed as multiple virtual IPs
from 192.168.2.0 to 192.168.2.0	
5. Global IP: 192.168.2.0	is transformed as multiple virtual IPs
from 192.168.2.0 to 192.168.2.0	
6. Global IP: 192.168.2.0	is transformed as multiple virtual IPs

Allows one or more public IP addresses to be shared by multiple internal users. Enter the Public IP address you wish to share into the Global IP field. Enter a range of internal IPs that will share the global IP.

Virtual Server

Virtual Server

You can configure the Wireless Barricade as a virtual server so that remote users accessing services such as the Web or FTP at your local site via public IP addresses can be automatically redirected to local servers configured with private IP addresses. In other words, depending on the requested service (TCP/UDP port number), the Wireless Barricade redirects the external service request to the appropriate server (located at another internal IP address).

	Private IP	Service Port	Type	Enabled
1.	192.168.2. <input type="text"/>	<input type="text"/>	TCP	<input type="checkbox"/>
2.	192.168.2. <input type="text"/>	<input type="text"/>	TCP	<input type="checkbox"/>
3.	192.168.2. <input type="text"/>	<input type="text"/>	TCP	<input type="checkbox"/>
4.	192.168.2. <input type="text"/>	<input type="text"/>	TCP	<input type="checkbox"/>
5.	192.168.2. <input type="text"/>	<input type="text"/>	TCP	<input type="checkbox"/>
6.	192.168.2. <input type="text"/>	<input type="text"/>	TCP	<input type="checkbox"/>
7.	192.168.2. <input type="text"/>	<input type="text"/>	TCP	<input type="checkbox"/>
8.	192.168.2. <input type="text"/>	<input type="text"/>	TCP	<input type="checkbox"/>
9.	192.168.2. <input type="text"/>	<input type="text"/>	TCP	<input type="checkbox"/>
10.	192.168.2. <input type="text"/>	<input type="text"/>	TCP	<input type="checkbox"/>

If you configure the Wireless Barricade as a virtual server, remote users accessing services such as Web or FTP at your local site via public IP addresses can be automatically redirected to local servers configured with private IP addresses. In other words, depending on the requested service (TCP/UDP port number), the Wireless Barricade redirects the external service request to the appropriate server (located at another internal IP address).

For example, if you set Type/Public Port to TCP/80 (HTTP or Web) and the Private IP/Port to 192.168.2.2/80, then all HTTP requests from outside users will be transferred to 192.168.2.2 on port 80. Therefore, by just entering the IP Address provided by the ISP, Internet users can access the service they need at the local address to which you redirect them.

The more common TCP service ports include:

HTTP: 80, FTP: 21, Telnet: 23, and POP3: 110.

Configuring the Wireless Barricade Router

Special Applications

Some applications, such as Internet gaming, videoconferencing, Internet telephony and others, require multiple connections. These applications cannot work with Network Address Translation (NAT) enabled. If you need to run applications that require multiple connections, use the following screen to specify the additional public ports to be opened for each application.

The screenshot shows the 'Advanced Setup' page for SMC Networks. The left sidebar contains a navigation menu with options: System, WAN, LAN, Wireless, NAT (selected), Address Mapping, Virtual Server, Special Applications (highlighted), Firewall, DDNS, UPnP, Tools, and Status. The main content area is titled 'Special Applications' and includes a descriptive paragraph about applications requiring multiple connections. Below the text is a table with 5 columns: Trigger Port, Trigger Type, Public Port, Public Type, and Enabled. The table contains 9 rows, each with a number in the first column. The 'Trigger Type' column has a dropdown menu set to 'TCP'. The 'Public Type' column also has a dropdown menu set to 'TCP'. The 'Enabled' column has a checkbox. A note at the top of the table states: 'Note: The range of the Trigger Ports is from 0 to 65535.'

	Trigger Port	Trigger Type	Public Port	Public Type	Enabled
1.	<input type="text"/>	TCP	<input type="text"/>	TCP	<input type="checkbox"/>
2.	<input type="text"/>	TCP	<input type="text"/>	TCP	<input type="checkbox"/>
3.	<input type="text"/>	TCP	<input type="text"/>	TCP	<input type="checkbox"/>
4.	<input type="text"/>	TCP	<input type="text"/>	TCP	<input type="checkbox"/>
5.	<input type="text"/>	TCP	<input type="text"/>	TCP	<input type="checkbox"/>
6.	<input type="text"/>	TCP	<input type="text"/>	TCP	<input type="checkbox"/>
7.	<input type="text"/>	TCP	<input type="text"/>	TCP	<input type="checkbox"/>
8.	<input type="text"/>	TCP	<input type="text"/>	TCP	<input type="checkbox"/>
9.	<input type="text"/>	TCP	<input type="text"/>	TCP	<input type="checkbox"/>

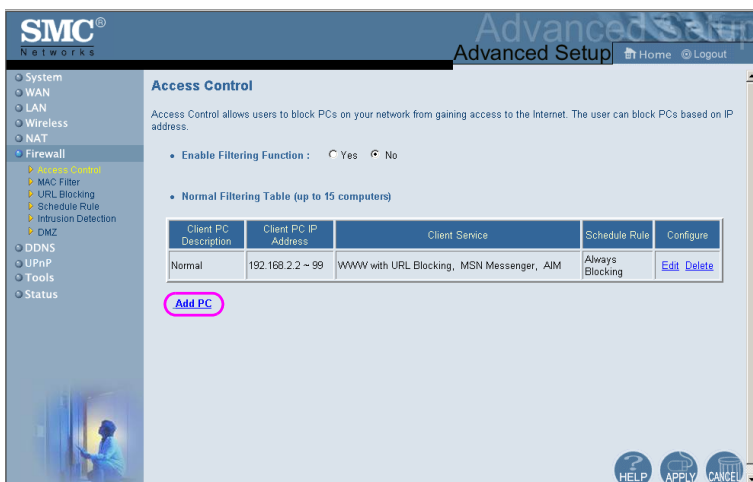
Specify the public port number normally associated with an application in the Trigger Port field. Set the protocol type to TCP or UDP, then enter the ports that the application requires. The ports may be in the format 7, 11, 57, or in a range, e.g., 72-96, or a combination of both, e.g., 7, 11, 57, 72-96.

For a full list of ports and the services that run on them, see www.iana.org/assignments/port-numbers.

Firewall

The Wireless Barricade firewall can provide access control of connected client PCs, block common hacker attacks, including IP Spoofing, Land Attack, Ping of Death, IP with zero length, Smurf Attack, UDP port loopback, Snork Attack, TCP null scan, and TCP SYN flooding. The firewall does not significantly affect system performance, so we advise leaving it enabled to protect your network users.

Access Control



SMC® Networks Advanced Setup [Home](#) [Logout](#)

- System
- WAN
- LAN
- Wireless
- NAT
- Firewall**
 - Wireless Firewall
 - MAC Filter
 - URL Blocking
 - Schedule Rule
 - Intrusion Detection
 - DMZ
- DDNS
- UPnP
- Tools
- Status

Access Control

Access Control allows users to block PCs on your network from gaining access to the Internet. The user can block PCs based on IP address.

• Enable Filtering Function : ☐ Yes ☒ No

• Normal Filtering Table (up to 15 computers)

Client PC Description	Client PC IP Address	Client Service	Schedule Rule	Configure
Normal	192.168.2.2 - 99	WWW with URL Blocking, MSN Messenger, AIM	Always Blocking	Edit Delete

[Add PC](#)

[HELP](#) [APPLY](#) [CANCEL](#)

Using this option allows you to specify different privileges based on IP address for the client PCs.

Configuring the Wireless Barricade Router

Note: Click on Add PC and define the appropriate settings for client PC services (as shown in the following screen).

SMC®
NETWORKS

Advanced Setup
Home Logout

System

WAN

LAN

Wireless

NAT

Firewall

Access Control

MAC Filter

URL Blocking

Schedule Rule

Intrusion Detection

DMZ

DDNS

UPnP

Tools

Status

Access Control Add PC

This page allows users to define service limitations of client PCs, including IP address, service type and scheduling rule criteria. For the URL blocking function, you need to configure the URL address first on the "URL Blocking Site" page. For the scheduling function, you also need to configure the schedule rule first on the "Schedule Rule" page.

Client PC Description: Normal

Client PC IP Address: 192.168.2.2 ~ 39

Client PC Service:

Service Name	Detail Description	Blocking
WWW	HTTP, TCP Port 80, 3128, 8000, 8080, 8081	<input type="checkbox"/>
WWW with URL Blocking	HTTP (Ref. URL Blocking Site Page)	<input checked="" type="checkbox"/>
E-mail Sending	SMTP, TCP Port 25	<input type="checkbox"/>
News Forums	NNTP, TCP Port 119	<input type="checkbox"/>
E-mail Receiving	POP3, TCP Port 110	<input type="checkbox"/>
Secure HTTP	HTTPS, TCP Port 443	<input type="checkbox"/>
File Transfer	FTP, TCP Port 21	<input type="checkbox"/>
MSN Messenger	TCP Port 1863	<input checked="" type="checkbox"/>
Telnet Service	TCP Port 23	<input type="checkbox"/>
AIM	AOL Instant Messenger, TCP Port 5190	<input checked="" type="checkbox"/>
NetMeeting	H.323, TCP Port 1720	<input type="checkbox"/>
DNS	UDP Port 53	<input type="checkbox"/>
SNMP	UDP Port 161, 162	<input type="checkbox"/>
VPN-PPPTP	TCP Port 1723	<input type="checkbox"/>
VPN-L2TP	UDP Port 1701	<input type="checkbox"/>
TCP	All TCP Port	<input type="checkbox"/>
UDP	All UDP Port	<input type="checkbox"/>

User Define Service

Protocol: ☒ TCP ☐ UDP

Port Range: 0 ~ 0, 0 ~ 0, 0 ~ 0, 0 ~ 0, 0 ~ 0, 0 ~ 0, 0 ~ 0, 0 ~ 0

Scheduling Rule (Ref. Schedule Rule Page): Always Blocking

OK Cancel

MAC Filtering Table

SMC®
Networks

Advanced Setup

Home Logout

System

WAN

LAN

Wireless

NAT

Firewall

- Access Control
- URL Blocking
- Schedule Rule
- Intrusion Detection
- DMZ

DDNS

UPnP

Tools

Status

MAC Filtering Table

This section helps provides MAC Filter configuration. When enabled, only MAC addresses configured will have access to your network. All other client devices will get denied access. This security feature can support up to 32 devices and applies to clients.

MAC Address Control :

☐ Yes ☒ No

MAC Filtering Table (up to 32 computers)

ID	Client PC MAC Address							
1		:		:		:		:
2		:		:		:		:
3		:		:		:		:
4		:		:		:		:
5		:		:		:		:
6		:		:		:		:
7		:		:		:		:
8		:		:		:		:
9		:		:		:		:
10		:		:		:		:
11		:		:		:		:
12		:		:		:		:

The MAC Filtering feature of the Wireless Barricade allows you to control access to your network to up to 32 clients based on the MAC (Media Access Control) Address of the client machine. This ID is unique to each network adapter. If the MAC address is listed in the table, that client machine will have access to the network.

Configuring the Wireless Barricade Router

URL Blocking

To configure the URL Blocking feature, use the table below to specify the websites (www.somesite.com) and/or keywords you want to filter on your network.

To complete this configuration, you will need to create or modify an access rule in “Access Control” on page 51. To modify an existing rule, click the Edit option next to the rule you want to modify. To create a new rule, click on the Add PC option.

From the Access Control Add PC section check the option for WWW with URL Blocking in the Client PC Service table to filter out the websites and keywords specified below.

SMC[®]
Networks

Advanced Setup

Home Logout

System

WAN

LAN

Wireless

NAT

Firewall

Access Control

MAC Filter

URL Blocking

Schedule Rule

Intrusion Detection

DMZ

DDNS

UPnP

Tools

Status

URL Blocking

Disallowed Web Sites and Keywords.

You can block access to certain Web sites from a particular PC by entering either a full URL address or just a keyword of the Web site.

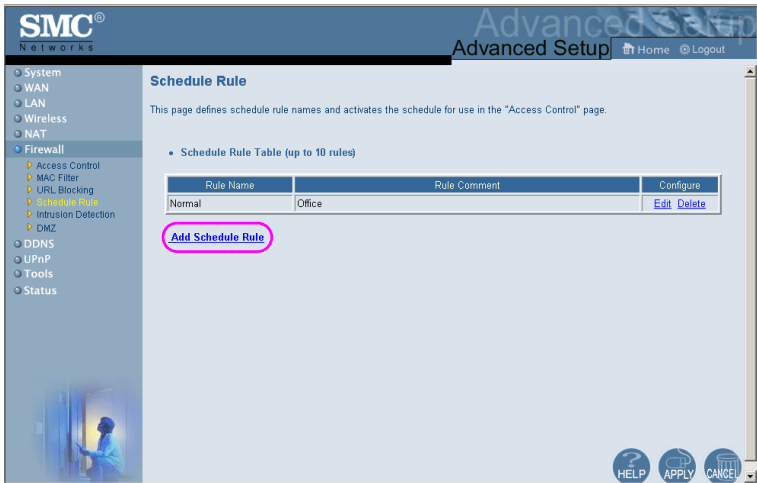
To specify the particular PC, go back to the "Access Control" page and check the box for "Http with URL Blocking" in the "Normal Filtering Table".

Rule Number	URL / Keyword	Rule Number	URL / Keyword
Site 1		Site 16	
Site 2		Site 17	
Site 3		Site 18	
Site 4		Site 19	
Site 5		Site 20	
Site 6		Site 21	
Site 7		Site 22	
Site 8		Site 23	
Site 9		Site 24	
Site 10		Site 25	
Site 11		Site 26	
Site 12		Site 27	

Use the above screen to block access to Web sites or to Web URLs containing the keyword specified in the table.

Schedule Rule

The Schedule Rule feature allows you to configure specific rules based on Time and Date. These rules can then be used to configure more specific Access Control.



Enables Schedule-based Internet access control.

1. Click Add Schedule Rule.
2. Define the settings for the schedule rule (as shown on the following screen).
3. Click OK and then click the APPLY button to save your settings.

Configuring the Wireless Barricade Router

SMC®
Networks

Advanced Setup
Advanced Setup Home Logout

System
WAN
LAN
Wireless
NAT
Firewall
Access Control
MAC Filter
URL Blocking
Schedule Rule
Intrusion Detection
DMZ
DDNS
UPnP
Tools
Status

Edit Schedule Rule

Use this section to create your network schedule rules.

The times you set below are the times periods that you want the Access Control Rule to be active. For example, if you want to block Internet access (block WWW) from 9AM to 9PM during the week. Simply configure 9:00 AM as "Start Time" and 9:00 PM as "End Time" for each weekday - during that time period the user will be unable to access the internet.

Once the schedule rule is setup, you will need to configure or edit an Access Control rule, and select your Schedule Rule that you want to apply to that Access Control rule. You can set the schedule rule at the bottom of the Access Control Configuration page in the "Scheduling Rule" drop-down option.

Schedule Rule Name

Schedule Rule Comment/Desc.

(ex. 10:30AM - 7:45PM)

Current Router Time

Wed Apr 30 05:25:17 2003

Week Day	Start Time (hh:mm)	End Time (hh:mm)
Every Day	<div></div> : <div></div> AM	<div></div> : <div></div> AM
Sunday	<div></div> : <div></div> AM	<div></div> : <div></div> AM
Monday	<div></div> : <div></div> AM	<div></div> : <div></div> AM
Tuesday	<div></div> : <div></div> AM	<div></div> : <div></div> AM
Wednesday	<div></div> : <div></div> AM	<div></div> : <div></div> AM
Thursday	<div></div> : <div></div> AM	<div></div> : <div></div> AM
Friday	<div></div> : <div></div> AM	<div></div> : <div></div> AM

Use this section to create your network schedule rules.

The times you set below are the times periods that you want the Access Control Rule to be active. For example, if you want to block Internet access (block WWW) from 9AM to 9PM during the week. Simply configure 9:00 AM as "Start Time" and 9:00 PM as "End Time" for each weekday - during that time period the user will be unable to access the internet.

Once the schedule rule is setup, you will need to configure or edit an Access Control rule, and select your Schedule Rule that you want to apply to that Access Control rule. You can set the schedule rule at the bottom of the Access Control Configuration page in the "Scheduling Rule" drop-down option.

Intrusion Detection

The screenshot shows the SMC Networks Advanced Setup web interface. On the left is a navigation menu with options: System, WAN, LAN, Wireless, NAT, Firewall (selected), DDNS, UPnP, Tools, and Status. The Firewall menu is expanded, showing sub-options: Access Control, MAC Filter, URL Blocking, Schedule Rule, Intrusion Detection (highlighted in yellow), and DMZ. The main content area is titled 'Intrusion Detection' and includes a descriptive paragraph: 'When the SPI (Stateful Packet Inspection) firewall feature is enabled, all packets can be blocked. Stateful Packet Inspection (SPI) allows full support of different application types that are using dynamic port numbers.' Below this are two configuration sections. The 'FIREWALL CONFIGURATION' section has two rows: 'SPI and Anti-DoS firewall protection' and 'Discard Ping From WAN', each with 'Enable' (selected) and 'Disable' radio buttons. The 'E-MAIL ALERT CONFIGURATION' section has four text input fields: 'Your E-mail Address', 'SMTP Server Address', 'User name', and 'Password'. At the bottom right are three buttons: HELP, APPLY, and CANCEL.

Firewall Configuration

- **SPI (Stateful Packet Inspection) and Anti-DoS firewall protection (Default: Enabled)** – the Wireless Barricade's Intrusion Detection feature limits access for incoming traffic at the WAN port. When the SPI feature is turned on, all incoming packets will be blocked.
- **Discard Ping from WAN (Default: Enabled)**
– Prevents a PING on the Wireless Barricade's WAN port from being routed to the network.

E-Mail Alert Configuration

- **When hackers attempt to enter your network, we can alert you by e-mail** – Enter your E-mail address. Specify your SMTP and POP3 servers, user name, and password.

Configuring the Wireless Barricade Router

DMZ (Demilitarized Zone)

SMC®
Networks

Advanced Setup

Home Logout

System

WAN

LAN

Wireless

NAT

Firewall

Access Control

MAC Filter

URL Blocking

Schedule Rule

Intrusion Detection

DMZ

DDNS

UPnP

Tools

Status

DMZ[Demilitarized Zone]

If you have a local client PC that cannot run an Internet application properly from behind the NAT firewall, then you can open the client up to unrestricted two-way Internet access by defining a Virtual DMZ Host.

Enable DMZ: ☒ Yes ☐ No

Multiple PCs can be exposed to the Internet for two-way communications e.g. Internet gaming, video conferencing, or VPN connections. To use the DMZ, you must set a static IP address for that PC.

Public IP Address	Client PC IP Address
1. 10.1.28.152	192.168.2.0
2. 0 0 0 0	192.168.2.0
3. 0 0 0 0	192.168.2.0
4. 0 0 0 0	192.168.2.0
5. 0 0 0 0	192.168.2.0
6. 0 0 0 0	192.168.2.0
7. 0 0 0 0	192.168.2.0
8. 0 0 0 0	192.168.2.0

HELP APPLY CANCEL

If you have a client PC that cannot run an Internet application properly from behind the firewall, then you can open the client up to unrestricted two-way Internet access. Enter the IP address of a DMZ host to this screen. Adding a client to the DMZ may expose your local network to a variety of security risks, so only use this option as a last resort.

DDNS (Dynamic DNS) Settings

SMC® Networks Advanced Setup [Home](#) [Logout](#)

- System
- WAN
- LAN
- Wireless
- NAT
- Firewall
- DDNS**
- UPnP
- Tools
- Status

DDNS (Dynamic DNS) Settings

Dynamic DNS provides users on the Internet a method to tie their domain name(s) to computers or servers. DDNS allows your domain name to follow your IP address automatically by having your DNS records changed when your IP address changes.

This DNS feature is powered by TZO.com. With a DDNS connection you can host your own web site, email server, FTP site and more at your own location even if you have a dynamic IP address. To sign-up for a free 30-day trial click [here](#)

Dynamic DNS: ☒ Enabled ☐ Disabled

TZO Configuration

Domain Name:

E-mail:

Key: [Get free 30-day trial key!](#)

Control Panel: [Click here to login to your TZO control panel](#)

Server Configuration

Server IP: 192.168.2.

Server Type:

Web Server:	(HTTP) Port 80 <input type="checkbox"/>	Port 8000 <input type="checkbox"/>
FTP Server:	Port 20 <input type="checkbox"/>	Port 21 <input type="checkbox"/>
Email Server:	(POP3) Port 110 <input type="checkbox"/>	(SMTP) Port 25 <input type="checkbox"/>

Domain Name is a series of alphanumeric strings separated by periods, that is the address of a network connection and that identifies the owner of the address.

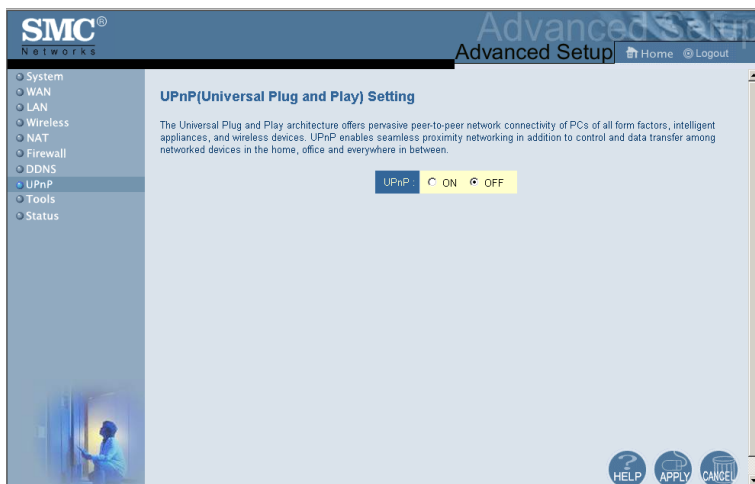
Dynamic DNS provides users on the Internet with a method to tie their domain name(s) to computers or servers. DDNS allows your domain name to follow your IP address automatically by having your DNS records changed when your IP address changes.

The Server Configuration section automatically opens the port options checked in the Virtual Server section. Simply enter in the IP Address of your server, such as a web server, and then click on the port option HTTP Port 80 so users can access your server from the WAN connection (Internet).

Configuring the Wireless Barricade Router

This DNS feature is powered by TZO.com. With a DDNS connection you can host your own web site, email server, FTP site, and more at your own location even if you have a dynamic IP address. (Default: Disable)

UPnP (Universal Plug and Play) Setting



Enable UPnP by checking ON in the screen above. UPnP allows the device to automatically:

- dynamically join a network
- obtain an IP address
- convey its capabilities and learn about the presence and capabilities of other devices.(Default: OFF)

Tools

Use the Tools menu to backup the current configuration, restore a previously saved configuration, restore factory settings, update firmware, and reset the Wireless Barricade.

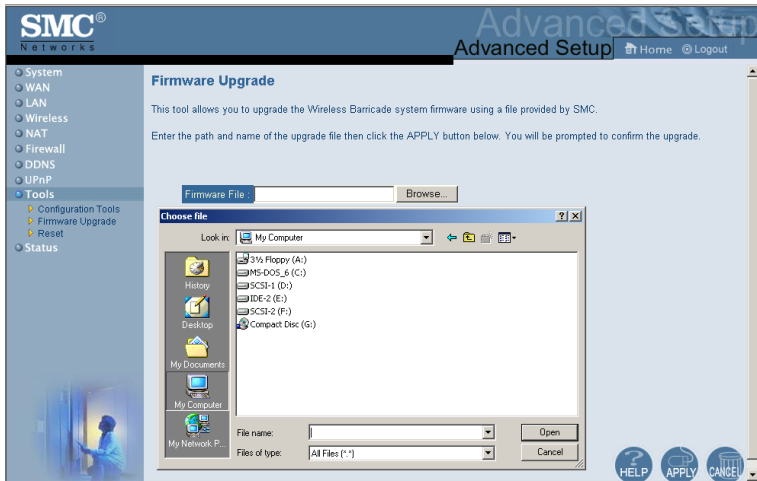
Tools - Configuration Tools



- Backup – saves the Wireless Barricade's configuration to a file.
- Restore – restores settings from a saved backup configuration file.
- Restore to factory defaults – restores the Wireless Barricade settings back to the factory default original.

Configuring the Wireless Barricade Router

Tools - Firmware Upgrade



Use this screen to update the firmware or user interface to the latest versions. Download the upgrade file from the SMC Web site (www.smc.com) and save it to your hard drive. In the Upgrade Target field, choose Firmware. Then click Browse to look for the previously downloaded file. Click APPLY. Check the Status page Information section to confirm that the upgrade process was successful.

Tools - Reset



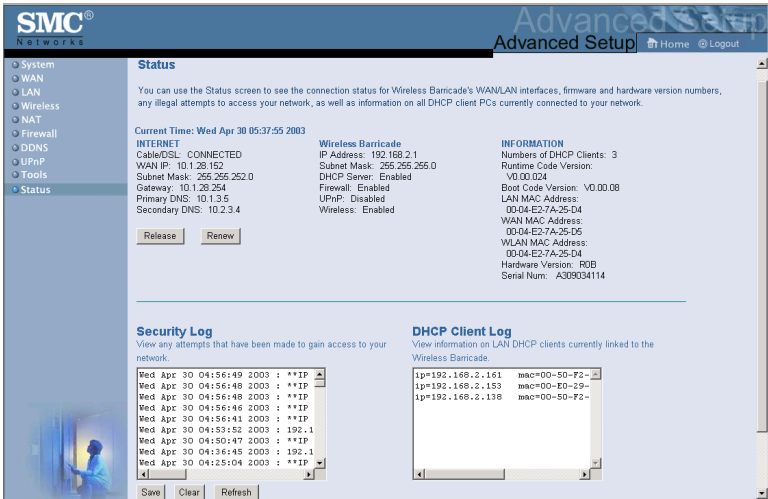
Click APPLY to reset the Wireless Barricade. The reset will be complete when the power LED stops blinking.

Note: If you use the Reset button on the front panel, the Wireless Barricade performs a power reset. If the button is held depressed for over five seconds, all the LEDs will illuminate and the factory settings will be restored.

Configuring the Wireless Barricade Router

Status

The Status screen displays WAN/LAN connection status, firmware, and hardware version numbers, illegal attempts to access your network, as well as information on DHCP clients connected to your network.



The following items are included on this screen:

Section	Description
INTERNET	Displays WAN connection type and status.
Wireless Barricade	Displays system IP settings, as well as DHCP, Firewall, UPnP and Wireless status.
INFORMATION	Displays the number of attached clients, the firmware versions, the physical MAC address for each media interface, as well as the hardware version and serial number.
Security Log	Displays illegal attempts to access your network.
Save	Click on this button to save the security log file.
Clear	Click on this button to delete the access log.
Refresh	Click on this button to refresh the screen.
DHCP Client Log	Displays information on all DHCP clients on your network.

TROUBLESHOOTING

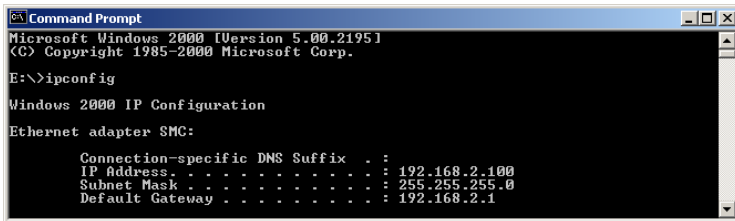
The information outlined in this section describes some useful steps for getting your computer and the Wireless Barricade Router online.

A. Verify your connection to the Wireless Barricade

If you are unable to access the Wireless Barricade's web-based administration pages then you may not be properly connected or configured. The screen shots in this section were taken on a Windows 2000 machine, but the same steps will apply to Windows 95/98/Me/XP.

To determine your TCP/IP configuration status please follow the steps below:

1. Click Start then choose Run.
2. Type cmd or command to open a DOS prompt.
3. In the DOS window, type ipconfig and verify the information that is displayed.
4. If your computer is setup for DHCP, then your TCP/IP configuration should be similar to the information displayed:
 - IP Address: 192.168.2.X (x is number between 100 and 199)
 - Subnet: 255.255.255.0
 - Gateway: 192.168.2.1



```
Command Prompt
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

E:\>ipconfig

Windows 2000 IP Configuration

Ethernet adapter SMC:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 192.168.2.100
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.2.1
```

If you have any other IP address information listed see below.

If you have an IP address that starts with 169.254.XXX.XXX then see the next section.

If you have another IP address configured, then see section C.

B. I am getting an IP Address that starts with 169.254.XXX.XXX

If you are getting this IP Address, then you need to check that you are properly connected to the Wireless Barricade.

Confirm that you have a good link light on the Wireless Barricade for the port this computer is connected to. If not, please try another cable.

If you have a good link light, please open up a DOS window as described in the previous section and type ipconfig/renew.

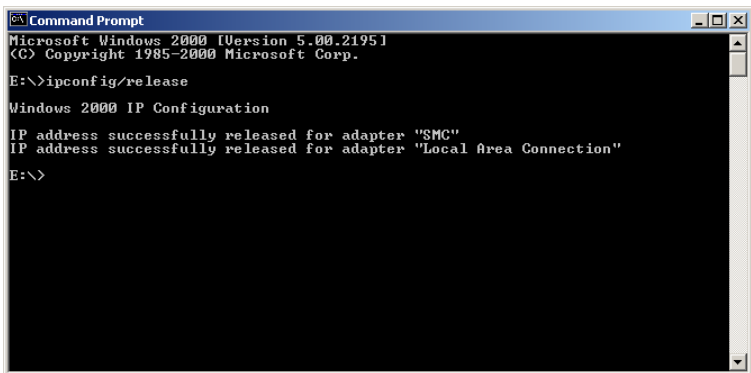
If you are still unable to get an IP Address from the Wireless Barricade, reinstall your network adapter. Please refer to your adapter manual for information on how to do this.

C. I have another IP Address displayed

If you have another IP address listed then the PC may not be configured for a DHCP connection. Please refer to “Configuring Client TCP/IP” on page 11 for information.

Once you have confirmed your computer is configured for DHCP, then please follow the steps below.

1. Open a DOS window as described above.
2. Type ipconfig/release.



```
Microsoft Windows [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

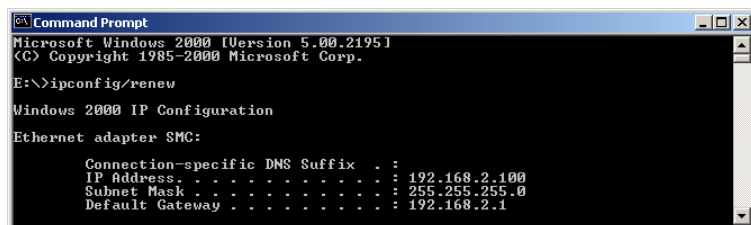
E:\>ipconfig/release

Windows 2000 IP Configuration

IP address successfully released for adapter "SMC"
IP address successfully released for adapter "Local Area Connection"

E:\>
```

3. Then type ipconfig/renew.



```
Microsoft Windows [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

E:\>ipconfig/renew

Windows 2000 IP Configuration

Ethernet adapter SMC:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 192.168.2.100
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.2.1
```

D. The 10/100 LED does not light after a connection is made.

1. Check that the host computer and hub are both powered on.
2. Be sure the network cable is connected to both devices.
3. Verify that Category 5 cable is used if you are operating at 100 Mbps, and that the length of any cable does not exceed 100 m (328 ft).
4. Check the network card connections.
5. The 10BASE-T/100BASE-TX hub/switch port, network card, or cable may be defective.

SPECIFICATIONS

Below is an outline of the Technical Specifications for the SMC7004VWBR

Standards

IEEE 802.3 10BASE-T Ethernet

IEEE 802.3u 100BASE-TX Fast Ethernet

IEEE 802.11b

LAN Interface

4 - RJ-45 10/100 Mbps Auto MDI/MDI-X ports

WAN Interface

1- RJ-45 10/100 Mbps Auto MDI/MDI-X port

Management

Web management

Advanced Features

Dynamic IP Address Configuration – DHCP, DNS

Firewall – Client privileges, hacker prevention and logging

Virtual Private Network – PPTP, L2TP, IPSec pass-through

Indicator Panel

Power, WLAN, WAN (Link, Activity), LAN (Link/Activity, 10/100 Mbps) LAN: Link/Activity, 10/100 (Mbps)

Temperature

Operating: 0 to 40 °C (32 to 104 °F)

Storage: -20 to 70 °C (-4 to 158 °F)

Dimensions

130 x 85 x 32 mm (5.12 x 3.35 x 1.26 in.)

Weight

370 g (13.05 oz)

Input Power

9 V (1 A)

Specifications

Internet Standards

ARP (RFC 826), IP (RFC 791), ICMP (RFC 792), UDP (RFC 768), TCP (RFC 793), Telnet (RFC 854-859), MD5 (RFC 1321), BOOTP Extension (RFC 1497), PPP LCP Extension (RFC 1570), PPPoE (RFC 2516), NAT (RFC 1631), PPP (RFC 1661), HTML (RFC 1866), HTTP (RFC 1945), CHAP (RFC 1944), DHCP (RFC 2131), PPTP (RFC 2637)

Temperature

Operating (0 to 40 °C), 32 to 104 °F

Storage (- 40 to 70 °C), - 40 to 158 °F

Humidity

5% to 95% (noncondensing)

Compliances

CE Mark

Emissions

FCC Class B

VCCI Class B

Industry Canada Class B

EN55022 (CISPR 22) Class B

C-Tick - AS/NZS 3548 (1995) Class B

Immunity

EN 61000-3-2/3

EN 61000-4-2/3/4/5/6/8/11

Safety

UL 1950

EN60950 (TÜV)

CSA 22.2 No. 950

FOR TECHNICAL SUPPORT, CALL:

From U.S.A. and Canada (24 hours a day, 7 days a week)
(800) SMC-4-YOU; (949) 679-8000; Fax: (949) 679-1481
From Europe (8:00 AM - 5:30 PM UK Time)
44 (0) 118 974 8700; Fax: 44 (0) 118 974 8701

INTERNET

E-mail addresses:

techsupport@smc.com
european.techsupport@smc-europe.com
support@smc-asia.com

Driver updates:

http://www.smc.com/index.cfm?action=tech_support_drivers_downloads

World Wide Web:

<http://www.smc.com>
<http://www.smc-europe.com>
<http://www.smc-asia.com>

FOR LITERATURE OR ADVERTISING RESPONSE, CALL:

U.S.A. and Canada:	(800) SMC-4-YOU;	Fax (949) 679-1481
Spain:	34-93-477-4935;	Fax 34-93-477-3774
UK:	44 (0) 1932 866553;	Fax 44 (0) 118 974 8701
France:	33 (0) 41 38 32 32;	Fax 33 (0) 41 38 01 58
Italy:	39 (0) 335 5708602;	Fax 39 02 739 14 17
Benelux:	31 33 455 72 88;	Fax 31 33 455 73 30
Central Europe:	49 (0) 89 92861-0;	Fax 49 (0) 89 92861-230
Nordic:	46 (0) 868 70700;	Fax 46 (0) 887 62 62
Eastern Europe:	34 -93-477-4920;	Fax 34 93 477 3774
Sub Saharian Africa:	27 0126610232;	Fax 27-11 314 9133
North West Africa:	216 71236616;	Fax 216 71751415
CIS:	7 (095) 789 35 73;	Fax 7 (095) 789 35 73
PRC (Beijing):	86-10-8251-1550;	Fax 86-10-8251-1551
PRC (Shanghai):	86-21-6485-9922;	Fax 86-21-6495-7924
Taiwan:	886-2-8797-8006;	Fax 886-2-8797-6288
Asia Pacific:	(65) 6 238 6556;	Fax (65) 6 238 6466
Korea:	82-2-553-0860;	Fax 82-2-553-7202
Japan:	81-3-5645-5715;	Fax 81-3-5645-5716
Australia:	61-2-8875-7887;	Fax 61-2-8875-7777
India:	91 22 5696 2790;	Fax 91 22 5696 2794
Middle East:	97 14 299 4466	Fax 97 14 299 4664
Thailand:	66 2 651 8733	Fax 66 2 651 8737

If you are looking for further contact information, please visit www.smc.com,
www.smc-europe.com, or www.smc-asia.com.

SMC®
Networks

38 Tesla

Irvine, CA 92618

Phone: (949) 679-8000

Model Number: SMC7004VWBR

Part Number: 150000026400E

Revision Number E052003-R01 F 1.0